BLICATIONS DE L'INSTITUT DE STATISTIQUE
DE L'UNIVERSITÉ DE PARIS

MÉMOIRES ET CONFÉRENCES SUR LE CALCUL DES PROBABILITÉS,
LA STATISTIQUE THÉORIQUE ET APPLIQUÉE, L'ÉCONOMÉTRIE

Devi Datt JOSHI

L'INFORMATION EN STATISTIQUE MATHÉMATIQUE ET DANS LA THÉORIE DES COMMUNICATIONS

A. FUCHS

SUR L'INÉGALITÉ DE SLUTSKY

ANALYSE D'OUVRAGES

VOL. VIII - FASCICULE 2 - 1959

PARIS
11, Rue Pierre-Curie

BLICATIONS DE L'INSTITUT DE STATISTIQUE
DE L'UNIVERSITÉ DE PARIS

MÉMOIRES ET CONFÉRENCES SUR LE CALCUL DES PROBABILITÉS,
LA STATISTIQUE THÉORIQUE ET APPLIQUÉE, L'ÉCONOMÉTRIE

Devi Datt JOSHI

L'INFORMATION EN STATISTIQUE MATHÉMATIQUE ET DANS LA THÉORIE DES COMMUNICATIONS

A. FUCHS

SUR L'INÉGALITÉ DE SLUTSKY

ANALYSE D'OUVRAGES

VOL. VIII - FASCICULE 2 - 1959

PARIS

11, Rue Pierre-Curie

Toute la correspondance relative aux publications
doit être envoyée à l'adresse
INSTITUT DE STATISTIQUE DE L'UNIVERSITÉ DE PARIS
Institut Henri Poincaré - 11, Rue Pierre Curie - Paris (5e)

Les manuscrits doivent être envoyés à M. Daniel DUGUE
à l'adresse précédente.

L'INFORMATION EN STATISTIQUE MATHÉMATIQUE ET DANS LA THÉORIE DES COMMUNICATIONS

Devi Datt JOSHI



INTRODUCTION

La théorie de l'information a connu un essor rapide depuis la parution du mémoire fondamental de SHANNON. Née de l'étude du problème des communications, elle trouve des applications dans des domaines très différents comme la psychologie, la linguistique ou la génétique. André et Denis GABOR (1954) s'en sont même inspirés pour entreprendre un travail aussi délicat que l'élaboration d'une théorie mathématique de la liberté. Mais malgré cet essor rapide les fondements de cette théorie restaient assez obscurs . Différents auteurs parmi lesquels nous citerons FORTET (1951), Mc MILLAN (1953) et KHINTCHINE (1953, 1956) remédièrent à cet état de choses. Les deux articles de KHINTCHINE constituent, à notre avis, l'exposé le meilleur et le plus complet de la théorie de SHANNON.

Dans notre premier chapitre, introduction à la théorie de SHANNON, nous montrons que les deux concepts de base de la théorie, à savoir l'entropie et la capacité, sont liés à deux problèmes de codage différents, et qu'en ce qui concerne le théorème dit fondamental, c'est le concept de capacité qui est seul en jeu. A titre d'exemple, nous considérons le cas simple d'une ligne binaire symétrique pour lequel nous donnons une nouvelle démonstration du théorème fondamental.

Ce dernier ne traite que du comportement asymptotique du système. Selon ce théorème, il existe des codes tels que si la longueur des messages augmente suffisamment l'erreur de transmission diminue et disparait à la limite. Mais la démonstration de l'existence de tels codes ne résout en rien le problème pratique de leur construction. De ce point de vue pratique le cas le plus important (qui est aussi le cas le plus simple) est celui d'une ligne de transmission n'utilisant comme messages que les suites formées de deux symboles 0 et 1. La recherche des codes dans ce cas, appelée problème du codage binaire, est étudiée dans le chapitre II. Puisqu'il n'existe aucune étude systématique de ce problème, malgré le nombre assez grand de travaux qui lui ont été consacrés, il nous a semblé utile d'en reprendre l'étude dès

la forme originelle dans laquelle il a été posé pour la première fois par HAMMING (1950). Il s'agit en effet de considérer l'espace des messages comme un groupe abélien d'ordre 2^n et du type (1, 1, . . . , 1). On définit sur ce groupe une métrique et le problème du codage devient la recherche des sous-ensembles tels que la distance entre deux éléments quelconques de ce sous-ensemble soit supérieure ou égale à un nombre déterminé, (code à distance donnée). On définit ensuite le code optimal. Nous avons démontré qu'il existe toujours un code optimal qui soit un sous-groupe. L'étude des propriétés de ces codes particuliers qui sont des sous-groupes révèle la liaison entre le problème du codage et celui de la décomposition des groupes abéliens du type considéré. En effet tout théorème sur la décomposition aurait son analogue pour le problème du codage. Deux théorèmes de cet ordre dus à ZAREMBA (1952) sont considérés à titre d'exemple. Le chapitre se termine par deux inégalités nouvelles sur le nombre d'éléments du code optimal le plus grand. Ces inégalités sont plus simples et la seconde donne des résultats beaucoup plus précis que ceux connus jusqu'à présent.

Dans le chapitre III nous envisageons la possibilité de généraliser la théorie de SHANNON aux espaces abstraits. Nous définissons une ligne de transmission comme un espace mesurable $(Y, \mathcal{Y})$ sur lequel est définie une mesure de probabilité ν_x pour tout point x appartenant à un autre espace mesurable $(X, \mathcal{X})$. La capacité d'une ligne est définie en général à partir de la fonction d'entropie. Or il n'est pas possible de définir l'entropie dans le cas général étudié ici. Une définition de la capacité qui ne ferait pas intervenir la fonction d'entropie est pourtant possible et elle constitue le point de départ de ce chapitre. Ayant ainsi défini la capacité nous démontrons un théorème analogue au théorème fondamental de SHANNON.

Le dernier chapitre est consacré à un examen de la notion d'information en statistique mathématique. L'information de FISHER était déjà connue des statisticiens mais c'est la théorie de SHANNON-WIENER (et surtout la remarque de WIENER (1948, p. 76) que son information pourrait remplacer celle de FISHER) qui a attiré l'attention sur le concept même. Plusieurs auteurs ont essayé de montrer l'unité entre l'information de FISHER et celle de SHANNON-WIENER. SCHUTZENBERGER (1954), allant plus loin a démontré que "toute information est la valeur moyenne, étendue à l'ensemble des états de la résultante d'un opérateur linéaire S sur le logarithme de la probabilité à priori de chaque état. . . . L'opérateur S doit être tel que l'information correspondante soit toujours positive ou nulle". (p. 43). La théorie de SCHUTZENBERGER quoique menant à des résultats d'une extrême généralité, a le défaut, comme toute théorie axiomatique de l'information (voir par exemple BARNARD (1951)), d'imposer des conditions trop restrictives au départ et de ne traiter que du cas discret. Nous avons donc réétudié cette question d'un point de vue différent.

Par analogie avec l'information de FISHER, nous considérons toute information comme une fonction numérique positive, définie par rapport à un espace mesurable (appelé espace d'observation), additive pour les observations indépendantes et invariante sous les transformations qui sont des résumés exhaustifs. Ce ne sont là que des propriétés générales et, pour qu'elle ait un sens en statistique mathématique, l'information doit avoir, en plus, le caractère d'un "renseignement" sur un problème précis. Prenons l'information de FISHER ; elle a, à part ces propriétés générales, une signification importante pour le problème de l'estimation des paramètres ; elle nous renseigne sur la précision que l'on peut atteindre. Mais l'information de FISHER perd ce caractère d'un renseignement dès qu'il s'agit d'un problème autre que celui de l'estimation. Il était donc utile de voir qu'il n'existerait pas des fonctions qui tout en ayant les propriétés générales d'une information apporteraient aussi des "renseignements" sur d'autres problèmes de statistique mathématique.

Deux cas ont été étudiés, celui du test d'hypothèse et celui de la discrimination. Nous avons démontré que l'information de SHANNON-WIENER pourrait être utilisée comme information de test d'hypothèse, et la fonction de "divergence" entre deux lois de probabilité proposée par CHERNOFF (1952) comme information de discrimination. Signalons que cette dernière ne revêt pas la forme générale d'une information telle que l'a énoncée SCHUTZENBERGER.

CHAPITRE I

LE THÉORÈME FONDAMENTAL DE LA THÉORIE DE L'INFORMATION : CAS DISCRET

LA NOTION D'ENTROPIE :

Soit $\mathcal{A}$ une épreuve et soient : $A_1, A_2, \ldots, A_n$ les évènements aléatoires liés à $\mathcal{A}$ et formant un système exhaustif. Si :

$$p_i = \Pr(A_i), \quad i = 1, 2, \ldots, n \quad p_i \geqslant 0, \quad \sum_i p_i = 1$$

sont les probabilités des évènements A_i, on appelle entropie du système $\mathcal{A}$ la quantité :

$$H(\mathcal{A}) = - \sum_i p_i \operatorname{Log} p_i$$

On sait que $H = 0$ si, et seulement si, toutes les probabilités p_i sauf une sont égales à zéro et que H est positive dans tous les autres cas. D'autre part, pour une valeur donnée de n, H atteint son maximum pour :

$$p_1 = p_2 = \ldots = p_n = 1/n$$

et dans ce cas : $H = \operatorname{Log} n.$

Soient $\mathcal{A}$ et $\mathcal{B}$ deux épreuves et soient :

$$A_1, A_2, \ldots, A_m$$

$$B_1, B_2, \ldots, B_n$$

les évènements aléatoires liés respectivement à $\mathcal{A}$ et à $\mathcal{B}$.

Désignons par $\mathcal{A}\,\mathcal{B}$ l'épreuve composée ayant pour évènements aléatoires liés, les évènements composés :

$$A_i B_j \; ; \quad i = 1, 2, \ldots, m \; ; \quad j = 1, 2, \ldots, n.$$

Désignons par $H(\mathcal{A})$, $H(\mathcal{B})$ et $H(\mathcal{A}\mathcal{B})$ les trois entropies correspondantes. Alors si les épreuves $\mathcal{A}$ et $\mathcal{B}$ sont indépendantes, telles que ·

$$Pr(A_i B_j) = Pr(A_i)\, Pr(B_j) \quad , \qquad \text{on a :}$$

$$H(\mathcal{A}\mathcal{B}) = H(\mathcal{A}) + H(\mathcal{B}).$$

Par contre, si les épreuves $\mathcal{A}$ et $\mathcal{B}$ sont liées, et si l'on a :

$$Pr(A_i B_j) = Pr(A_i)\, Pr(B_j/A_i)$$

on définit l'entropie conditionnelle de $\mathcal{B}$ par rapport à $\mathcal{A}$ comme

$$H_{\mathcal{A}}(\mathcal{B}) = - \sum_i Pr(A_i) \sum_j Pr(B_j/A_i) \,\text{Log}\, Pr(B_j/A_i)$$

D'une façon analogue on définit l'entropie conditionnelle de $\mathcal{A}$ par rapport à $\mathcal{B}$, $H_{\mathcal{B}}(\mathcal{A})$ et on a :

$$H(\mathcal{A}\mathcal{B}) = H(\mathcal{A}) + H_{\mathcal{A}}(\mathcal{B}) = H(\mathcal{B}) + H_{\mathcal{B}}(\mathcal{A}).$$

La fonction d'entropie H possède des propriétés remarquables dont une des plus importantes est la suivante.

Soit $H(p_1, p_2, \ldots, p_n)$ une fonction continue par rapport à toutes ses variables, définie pour tout $p_i \geqslant 0$, $\sum_i p_i = 1$ et pour tout entier positif fini n. Si :

(i) pour toute valeur donnée de n, H atteint son maximum pour

$$p_1 = p_2 = \ldots = p_n = i/n$$

(ii) $H(\mathcal{A}\mathcal{B}) = H(\mathcal{A}) + H_{\mathcal{A}}(\mathcal{B})$ (dans le sens défini plus haut)

(iii) $H(p_1, p_2, \ldots, p_n, 0) = H(p_1, p_2, \ldots, p_n)$,

alors : $H(p_1, p_2, \ldots, p_n) = - \lambda \sum_i p_i \,\text{Log}\, p_i$

où λ est une constante positive. (Pour la démonstration voir Khintchine (1953)).

ENTROPIE D'UNE SOURCE :

Dans le langage de la théorie des communications, une source est un processus stochastique fini et discret. On appelle "alphabet" de la source l'ensemble fini A des états $a_1, a_2, \ldots, a_m$ que peut prendre le système. Les a_i sont des "lettres" de l'alphabet A, et les suites

formées de ces lettres constituent les "messages" ou la production de la source.

Soit n_0 un nombre entier positif donné, et considérons les suites :

$$x_{n_0},\ x_{n_0+1},\ \ldots,\ x_{n_0+n-1}\ ; \qquad x_i \in A.$$

Pour n_0 et n donnés, l'ensemble de toutes les suites de cette forme est un ensemble fini ayant m^n éléments. Cet ensemble a une loi de probabilité bien définie et possède donc une entropie. Soit $H(n_0, n)$ l'entropie de cet ensemble de probabilités. On définit alors l'entropie du processus à partir de l'instant n_0 comme :

$$H(n_0) = \lim_{n \to \infty} (1/n)\, H(n_0, n),$$

si cette limite existe.

Shannon dans son mémoire n'avait étudié que des sources qui sont des processus de Markoff réguliers pour lesquels l'entropie H est donnée par :

$$H = - \sum p_i\, p_{ij} \operatorname{Log} p_{ij},$$

où

$$\| p_{ij} \|$$

est la matrice des probabilités de transition, et les P_i sont des probabilités à priori.

Mc Millan (1953) a étendu cette définition à un processus discret fini ergodique (non-nécessairement markovien) sous l'hypothèse que le processus est en cours depuis $- \infty$. Il a démontré que sous l'hypothèse d'ergodisme le processus avait une entropie bien définie.

La définition que nous avons donnée ci-dessus est due à Fortet (1951). Remarquons que si le processus est stationnaire la limite $H(n_0)$ ne dépend pas de n_0 de telle sorte que nous pourrons parler tout simplement de l'entropie H de la source. En général on ne considère que les sources stationnaires. Leur importance est montrée par le théorème suivant dont la démonstration est empruntée à Khintchine (1956).

THEOREME I -

Toute source stationnaire possède une entropie.

Soit, en effet, A_{n+m} l'ensemble de tous les messages de longueur

$n + m$ (n, m arbitraires). Désignons par $H(A_r)$ l'entropie de l'ensemble A_r. Sous l'hypothèse de stationnarité, cette entropie est une fonction de r seulement. On a évidemment :

$$H(A_{n+m}) = H(A_n) + H_{A_n}(A_m)$$

et $H_{A_n}(A_m) \leqslant H(A_m)$, c'est-à-dire : $H(A_n) \leqslant H(A_{n+m}) \leqslant H(A_n) + H(A_m)$

que nous écrirons :

$$H_n \leqslant H_{n+m} \leqslant H_n + H_m \,. \quad \text{En particulier :}$$

$$H_n \leqslant H_{n+1} \quad \text{et} \quad H_{kn} \leqslant k\, H_n \,,$$

k étant un nombre entier positif quelconque. Et finalement :

$$(1/k)\, H_k \leqslant H_1$$

ce qui démontre que :

$$\operatorname*{Lim\,Inf}_{n \to \infty} (1/n)\, H_n \quad \text{existe. Soit :}$$

$$\operatorname*{Lim\,Inf}_{n \to \infty} (1/n)\, H_n = a < +\infty.$$

Pour un nombre positif ε arbitrairement petit on peut choisir un indice q tel que :

$$(1/q)\, H_q < a + \varepsilon$$

Soient maintenant $n > q$, et k le nombre entier positif défini par

$$(k - 1)q < n \leqslant kq.$$

On a alors : $H_n \leqslant H_{kq}$, c'est-à-dire :

$$(1/n)H_n \leqslant \frac{H_{kq}}{(k-1)q} \leqslant \frac{k}{(k-1)} \frac{H_q}{q} \quad \text{car} \quad H_{kq} \leqslant kH_q.$$

Par conséquent, pour n suffisamment grand,

$$(a - \varepsilon) < \frac{H_n}{n} \leqslant \frac{k}{(k-1)} \frac{H_q}{q} < \frac{k}{(k-1)} (a + \varepsilon) < (a + 2\varepsilon)\,.$$

Comme ε est arbitrairement petit, on a :

$$\operatorname*{Lim}_{n \to \infty} (1/n)\, H_n = a$$

et le théorème est démontré.

Nous voyons donc que pour que l'entropie existe il suffit que la source soit stationnaire. Pourtant, pour la théorie des communications il faut supposer, en outre, que la source est ergodique. En ce qui concerne les applications, l'ergodisme est la propriété la plus importante. Les sources ergodiques possèdent ce que nous appellerons d'après Mc Millan la propriété de répartition asymptotique uniforme ("Asymptotic equi-partition property"). Cette propriété est énoncée dans le théorème suivant.

THEOREME 2 -

Soient ε, η deux nombres positifs arbitrairement petits. Pour n suffisamment grand les messages de longueur n d'une source d'entropie H se répartissent en deux catégories. Pour tout message C de la première catégorie (appelé message de probabilité forte) on a :

$$\left| \frac{\text{Log } Pr(C)}{n} + H \right| < \varepsilon \quad ;$$

L'ensemble des messages de la seconde catégorie (appelés messages de probabilité faible) a une probabilité inférieure à η.

En effet, on démontre que sous l'hypothèse d'ergodisme les fonctions :

$$f_n = -(1/n) \text{ Log } Pr(C)$$

tendent en probabilité vers H, d'où le théorème.

L'importance de ce théorème réside en ceci : Etant donnée une source ergodique d'entropie H, pour n suffisamment grand, parmi les messages de longueur n, on n'a qu'à considérer les messages de la première catégorie. Ces messages ont tous, approximativement, la même probabilité a^{-nH}, et leur nombre est donc à peu près égal à a^{nH}, a étant la base du système de logarithmes adopté.

La propriété de répartition asymptotique uniforme conduit à ce que nous appellerons le premier problème du codage, pour le distinguer du problème du codage lié à la notion de capacité d'une ligne de transmission. Celui-ci sera appelé le second problème du codage. Il est nécessaire de faire cette distinction car les deux méthodes répondent à deux exigences différentes, la première à celle d'économie, la seconde à celle de la réduction de l'erreur d'identification.

Supposons que l'on ait une source d'entropie H ayant pour l'alphabet A les m lettres :

$$a_1, a_2, \ldots, a_m$$

et un autre alphabet B ayant s lettres :

$$b_1, b_2, \ldots, b_s.$$

Le premier problème du codage est un problème de "traduction". Il s'agit d'établir une correspondance bi-univoque entre les messages-A et les messages-B, c'est-à-dire entre les suites formées des symboles a_i et les suites formées des symboles b_j, telle que la longueur moyenne des messages-B soit aussi petite que possible. C'est ce que nous avons appelé l'exigence d'économie.

Considérons les suites C_A de longueur n de la forme :

$$x_1, x_2, \ldots, x_n; \quad x_i \in A.$$

Supposons que notre code associe à chacune de ces suites C_A une suite de la forme :

$$y_1, y_2, \ldots, y_N; \quad y_j \in B \quad \text{de longueur } N(C_A).$$

Nous appellerons coefficient de contraction (cf. Khintchine (1953)) la quantité :

$$\mu = \lim_{n \to \infty} (1/n) \sum_{C_A} Pr(C_A)\, N(C_A)$$

Nous avons alors le théorème suivant :

THEOREME 3 -

Pour tout code, on a :

$$\mu \geqslant H/(\text{Log } s) \quad ,$$

et pour tout nombre positif arbitrairement petit η il existe un code tel que :

$$\mu < (H + \eta)/(\text{Log } s).$$

Remarquons que dans le cas où s (le nombre de lettres dans l'alphabet B) est égal à m, la borne inférieure du coefficient de contraction est égal à H/(Log m). Le dénominateur est la valeur maximum de H, et cette quantité est donc aussi appelée le rapport d'entropie ("entropy ratio").

D'habitude on n'énonce ce théorème que pour le cas où les deux alphabets A et B ont le même nombre de lettres, mais la démonstration (cf. Khintchine (1953)) s'étend facilement au cas ci-dessus.

Avant d'en arriver au second problème du codage il nous faut définir la notion de capacité d'une ligne de transmission.

CAPACITE D'UNE LIGNE DE TRANSMISSION :

Une ligne de transmission est un système constitué par :

(i) Un ensemble fini A d'éléments : $a_1, a_2, \ldots, a_r$;

(ii) Un ensemble fini B d'éléments : $b_1, b_2, \ldots, b_s$;

(iii) Une famille de lois de probabilité conditionnelle : $Pr(b_j/a_i)$

définies pour tout $a_i \in A$ et pour tout $b_j \in B$. L'ensemble A est appelé l'alphabet à l'entrée ; de même B est appelé l'alphabet à la sortie. Les suites de lettres a_i et b_j forment respectivement les messages à l'entrée et à la sortie. La famille de lois de probabilité conditionnelle constitue le "bruit" qui fait que tout message transmis est défiguré par ce bruit selon la loi de probabilité qui le définit.

Si maintenant les lettres a_i sont choisies selon une loi de probabilité donnée, soit :

$$P = \{ p_1, \ldots, pr \} \quad ; \quad p_i = Pr(a_i) \ ,$$

on peut définir les entropies $H(A)$, $H(B)$, $H_A(B)$, $H_B(A)$ et $H(AB)$.

On appelle débit de transmission la quantité :

$$\begin{aligned} R(P) &= H(A) + H(B) - H(AB) \\ &= H(A) - H_B(A) \\ &= H(B) - H_A(B). \end{aligned}$$

Soit maintenant $\mathfrak{P}$ la classe de toutes les lois de probabilité P que l'on peut définir sur l'ensemble A. Cette classe dépendra évidemment de la ligne. On appelle capacité de la ligne la quantité :

$$C = \operatorname*{Sup}_{P \in \mathfrak{P}} R(P)$$

Considérons maintenant les messages à l'entrée et à la sortie, c'est-à-dire les suites de la forme :

$$x_1, x_2, \ldots, x_n \quad ; \quad x_i \in A$$

$$y_1, y_2, \ldots, y_n \quad ; \quad y_j \in B$$

Nous supposerons que les x_i d'un message à l'entrée sont choisis indépendamment l'un de l'autre. Tout message :

$$x = (x_1, x_2, \ldots , x_n)$$

définit une probabilité conditionnelle sur l'ensemble des messages

$$y = (y_1, y_2, \ldots y_n)$$

Le problème qui se pose maintenant est de trouver une méthode qui permettrait pour tout message y à la sortie d'identifier le message x à l'entrée de telle sorte que l'erreur d'identification soit réduite au minimum. C'est en quoi consiste le second problème du codage.

Plus précisément, si $\mathcal{A}_n$ est l'ensemble de tous les messages de longueur n à l'entrée, on croit qu'en se limitant à l'emploi d'une partie seulement des messages possibles $\mathcal{A}_n$ on peut réduire l'erreur. En d'autres termes on croit pouvoir augmenter l'efficacité d'identification en faisant sacrifice de l'économie.

Le problème est donc de choisir un sous-ensemble $\mathcal{A}_n^*$ de $\mathcal{A}_n$ tel que, si les messages à l'entrée sont soumis à la condition d'appartenir à $\mathcal{A}_n^*$, on puisse, en prenant n suffisamment grand, rendre l'erreur d'identification aussi petite que l'on veut. Evidemment le choix de l'entier n et du sous-ensemble $\mathcal{A}_n^*$ dépendra de la méthode d'identification adoptée d'une part et du niveau de certitude que l'on veut atteindre d'autre part.

L'importance de la notion de capacité pour ce second problème du codage est révélée par le théorème appelé, d'après Shannon, le théorème fondamental. Ce théorème a pour objet de démontrer qu'étant donné ε, un nombre positif arbitrairement petit, on peut choisir l'ensemble $\mathcal{A}_n^*$ tel que, pour n suffisamment grand, l'erreur d'identification soit inférieure à ε et que $(1/n)$ Log N soit aussi proche de la capacité C que l'on veut, N étant le nombre d'éléments de l'ensemble $\mathcal{A}_n^*$.

Shannon dans sa démonstration du théorème fondamental montre que l'on peut rendre l'erreur d'identification arbitrairement petite, en prenant n suffisamment grand, si parmi les messages $\mathcal{A}_n$ on choisit au hasard un nombre $N < a^{nC}$ (a étant la base du système de logarithmes) et que cela n'est pas possible pour $N > a^{nC}$. L'identification se fait d'après le principe du maximum de probabilité à posteriori, c'est-à-dire que pour tout message y à la sortie on prend comme message à l'entrée le message x pour lequel $Pr(x/y)$ est le maximum.

Feinstein (1954) a donné une autre démonstration. Le théorème démontré par lui est un théorème d'existence, c'est-à-dire qu'il ne fournit pas une méthode pour choisir le sous-ensemble $\mathcal{A}_n^*$. Il démontre simplement qu'il existe un sous-ensemble $\mathcal{A}_n^*$ de $\mathcal{A}_n$ tel que pour tout

message $x_i \in \mathcal{A}_n^*$ il existe un sous-ensemble E_i de l'ensemble des messages à la sortie ayant les propriétés suivantes :

(i) $E_i \cap E_j = \emptyset$, $i \neq j$,

(ii) $\Pr(E_i / x_i) > 1 - \varepsilon$, $\varepsilon > 0$ (arbitrairement petit)

et que le nombre d'éléments de $\mathcal{A}_n^*$ tend vers a^{nC} lorsque $n \longrightarrow \infty$. Tout message à la sortie appartenant à E_i étant supposé provenir de x_i on voit que l'erreur d'identification est inférieure à ε et ceci pour toute loi de probabilité à priori selon laquelle sont choisis les messages à l'entrée $x_i \in \mathcal{A}_n^*$.

Dans les énoncés du théorème fondamental que l'on trouve dans la littérature, on fait intervenir à la fois les deux notions, celle de l'entropie d'une source et celle de la capacité d'une ligne. On démontre que la production d'une source d'entropie H ne peut être transmise par une ligne de capacité C avec erreur arbitrairement petite que si $H \leqslant C$. Mais en fait toute démonstration se fait en deux étapes. On démontre d'abord que, pour n grand, on peut choisir un sous-ensemble de a^{nC} messages à l'entrée tel que l'identification de ces messages soit possible avec une erreur infiniment petite. Puis on démontre que l'on peut établir une correspondance bi-univoque entre la production de la source et ce sous-ensemble. Une condition implicite (mais à notre connaissance jamais exprimée) dans toutes ces démonstrations, c'est que cette correspondance est établie entre les messages de même longueur. Sous une telle condition, il est évident, d'après la propriété de répartition asymptotique uniforme (on ne s'occupera que des a^{nH} messages de probabilité forte), que cette correspondance ne peut s'établir que pour $H \leqslant C$.

LA LIGNE BINAIRE SYMETRIQUE :

Nous donnerons maintenant une démonstration du théorème fondamental pour le cas d'une ligne binaire symétrique. Ce cas, le plus simple, est aussi le plus important pour les applications.

L'espace des messages transmis et celui des messages reçus est constitué alors par les suites de longueur n formées de deux symboles 0 et 1. Pour n donné cet espace contient 2^n points ou éléments. La probabilité d'erreur est la même pour les deux symboles, c'est-à-dire que la probabilité conditionnelle pour que le symbole 1 soit reçu lorsque 0 est transmis ou que 0 soit reçu lorsque 1 est transmis est la même. De plus cette probabilité est la même pour tous les n symboles de la suite qui constitue un message. D'où le nom de la ligne binaire symétrique. Comme il est de coutume dans ce cas, nous prendrons le nombre 2 comme base du système de logarithmes.

Désignons par C_n l'espace des messages et soient :

$$a_1, a_2, \ldots, a_\mu \quad ; \quad \mu = 2^n$$

les éléments de C_n. Soit p la probabilité d'erreur de transmission. Si l'on désigne par P_i^r la probabilité conditionnelle pour qu'il y ait au plus r ($\leqslant$ n) erreurs lorsque le message a_i est transmis, on a :

$$P_i^r = \sum_{m=0}^{r} \binom{n}{m} p^m (1-p)^{n-m}$$

On voit que cette probabilité ne dépend pas de a_i, le message transmis.

Soit maintenant E_i^r le sous-ensemble de C_n constitué par les suites qui ne diffèrent de la suite a_i que dans au plus r positions. E_i^r est donc l'ensemble des messages reçus lorsqu'il y a au plus r erreurs dans la transmission du message a_i. L'ensemble E_i^r contient :

$$\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{r}$$

éléments différents et on voit que P_i^r n'est que la probabilité conditionnelle qu'après la transmission du message a_i, le message reçu se trouve dans E_i^r ;

$$P_i^r = Pr(E_i^r / a_i)$$

Supposons maintenant que pour un nombre positif ε arbitrairement petit on choisit n et r tels que :

$$P_i^r > 1 - \varepsilon$$

Cela est toujours possible car, d'après le théorème de Bernoulli, on sait que pour $\lambda > p$:

$$\sum_{m=0}^{n\lambda} \binom{n}{m} p^m (1-p)^{n-m} \longrightarrow 1$$

lorsque $n \to \infty$. Supposons, en outre, qu'il existe des points $a_1, a_2, \ldots, a_N$ de C_n tels que les ensembles correspondants E_i^r sont deux à deux disjoints. Si ces N messages sont transmis avec une distribution arbitraire des probabilités à priori :

$$p_1, p_2, \ldots, p_N$$

et si l'on identifie tout message reçu appartenant à E_i^r avec a_i, l'erreur totale de décodage sera :

$$\sum_{i=1}^{N} p_i (1 - \hat{p}_i) < \sum_{i=1}^{N} p_i \; \varepsilon = \varepsilon .$$

c'est-à-dire que l'erreur totale sera inférieure à ε. Nous pouvons maintenant énoncer le théorème fondamental.

THEOREME 4 -

Soit C la capacité et soit $p < (1/2)$. Si $\tilde{N}$ est la borne supérieure de N

$$\lim_{n \to \infty} (1/n) \operatorname{Log} \tilde{N} = C$$

Notons d'abord que, pour n et r donnés, tout ensemble E_i^r contient :

$$\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{r}$$

points. La borne supérieure $\tilde{N}$ du nombre de points que l'on peut choisir tel que les ensembles correspondants E_i^r soient deux à deux disjoints, est donc donnée par :

$$\tilde{N} = \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{r}}$$

Or, nous avons, pour $r < (n/2)$:

$$\binom{n}{r} < \binom{n}{0} + \binom{n}{1} + \dots + \binom{n}{r} < \frac{n-r}{n-2r} \binom{n}{r}$$

Ainsi donc :

$$\frac{2^n}{\frac{n-r}{n-2r}\binom{n}{r}} < \tilde{N} < \frac{2^n}{\binom{n}{r}}$$

D'autre part, la capacité C est donnée par :

$$C = 1 + p \operatorname{Log} p + q \operatorname{Log} q, \quad q = 1 - p .$$

Nous avons supposé $p < (1/2)$. On peut donc choisir un nombre α $(p < \alpha < 1/2)$ tel que, pour un nombre positif arbitrairement petit η on ait :

$$C - \eta < C' = 1 + \alpha \operatorname{Log} \alpha + \beta \operatorname{Log} \beta < C, \quad \beta = 1 - \alpha$$

D'après le théorème de Bernoulli on a :

$$\lim_{n \to \infty} \sum_{m=0}^{n\alpha} \binom{n}{m} p^m q^{n-m} = 1 ,$$

c'est-à-dire qu'étant donné ε, un nombre positif arbitrairement petit, on peut trouver un nombre entier n_0, tel que :

$$\sum_{m=0}^{n\alpha} \binom{n}{m} p^m q^{n-m} > 1 - \varepsilon \qquad \text{pour tout } n \geqslant n_0 .$$

Donc pour ε donné, on peut choisir n puis $r = n\alpha$ tels que :

$$p_i^r > 1 - \varepsilon$$

$\tilde{N}$ étant définie comme plus haut, on a :

$$\frac{2^n}{\frac{\beta}{\beta - \alpha}\binom{n}{n\alpha}} < \tilde{N} < \frac{2^n}{\binom{n}{n\alpha}}$$

Si l'on prend les logarithmes (toujours à base 2), on a :

$$n - \operatorname{Log}\frac{\beta}{\beta - \alpha} - \operatorname{Log}\binom{n}{n\alpha} < \operatorname{Log}\tilde{N} < n - \operatorname{Log}\binom{n}{n\alpha}$$

Nous utiliserons ensuite l'approximation suivante (l'approximation de Stirling) :

$$(2\pi)^{1/2} n^{n+1/2} e^{-n} < n\,! < (2\pi)^{1/2}\left(n + \frac{1}{2}\right)^{n+1/2} e^{-(n+1/2)}$$

Cela donne :

$$- (1/2)(\operatorname{Log} e + \operatorname{Log} 2\pi) - (1/2)\operatorname{Log} n + (n + 1/2)\operatorname{Log}\left(1 + \frac{1}{2n}\right) -$$

$$- n(\alpha\operatorname{Log}\alpha + \beta\operatorname{Log}\beta) - (1/2)\operatorname{Log}\alpha\beta > \operatorname{Log}\binom{n}{n\alpha} > - (1/2)\operatorname{Log} 2\pi + \operatorname{Log} e -$$

$$- (1/2)\operatorname{Log} n - n(\alpha\operatorname{Log}\alpha + \beta\operatorname{Log}\beta) - (1/2)\operatorname{Log}\alpha\beta - \left(n\alpha + \frac{1}{2}\right)\operatorname{Log}\left(1 + \frac{1}{2n\alpha}\right) -$$

$$-\left(n\beta + \frac{1}{2}\right)\operatorname{Log}\left(1 + \frac{1}{2n\beta}\right)$$

Et finalement on a :

$$n(1 + \alpha\operatorname{Log}\alpha + \beta\operatorname{Log}\beta) - \operatorname{Log}\frac{\beta}{\beta - \alpha} + \frac{1}{2}(\operatorname{Log} e + \operatorname{Log} 2\pi) + \frac{1}{2}\operatorname{Log} n -$$

$$- (n + \frac{1}{2}) \text{Log} (1 + \frac{1}{2n}) + \frac{1}{2} \text{Log}\, \alpha\beta < \text{Log}\, \tilde{N} < n(1 + \alpha \text{Log}\, \alpha + \beta \text{Log}\, \beta) +$$

$$+ \frac{1}{2} \text{Log}\, 2\pi + \text{Log}\, e + \frac{1}{2} \text{Log}\, n + \frac{1}{2} \text{Log}\, \alpha\beta + (n\alpha + \frac{1}{2}) \text{Log} (1 + \frac{1}{2n\alpha}) +$$

$$+ (n\beta + \frac{1}{2}) \text{Log} (1 + \frac{1}{2n\beta}) .$$

En divisant par n et en mettant :

$$1 + \alpha \text{Log}\, \alpha + \beta \text{Log}\, \beta = C'$$

On obtient :

$$(k/n) + (1/2n) \text{Log}\, n - (1 + \frac{1}{2n}) \text{Log} (1 + \frac{1}{2n}) < (1/n) \text{Log}\, \tilde{N} - C' <$$

$$< (k'/n) + (1/2n) \text{Log}\, n + (\alpha + \frac{1}{2n}) \text{Log} (1 + \frac{1}{2n\alpha}) + (\beta + \frac{1}{2n}) \text{Log} (1 + \frac{1}{2n\beta}) ,$$

c'est-à-dire :

$$\lim_{n \to \infty} (1/n) \text{Log}\, N = C'$$

Mais on a :

$$C - \eta < C' < C$$

et comme η est arbitraire, on a :

$$\lim_{n \to \infty} (1/n) \text{Log}\, \tilde{N} = C$$

ce qui démontre le théorème.

Remarquons que nous avons seulement démontré que c'est la borne supérieure des messages que l'on peut choisir qui tend vers 2^{nC} et non pas le nombre de messages lui-même. Cela parce que nous n'avons pas donné un théorème d'existence, mais qu'au contraire nous avons fait dépendre notre démonstration de la méthode de choix des messages à l'entrée. Cette méthode nous conduit à considérer le problème du codage binaire (il s'agit évidemment du second problème du codage), qui fait l'objet du chapitre suivant.

CHAPITRE II

LE PROBLÈME DU CODAGE BINAIRE

L'ESPACE C_n ET LE CODE OPTIMAL -

Soit C_n l'ensemble de toutes les suites de longueur n formées de deux symboles 0 et 1. C_n contient donc 2^n éléments différents. Tout élément $\alpha \in C_n$ peut être représenté comme un vecteur à n composantes

$$\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \; ; \; \alpha_i = 0, 1 \; ; \; i = 1, 2, \ldots, n.$$

A tout élément $\alpha \in C_n$ on associe un nombre entier positif appelé la norme de α et définie par :

$$\| \alpha \| = \sum_{i=1}^{n} \alpha_i$$

Sur l'espace C_n on définit ensuite une distance

$$\delta(\alpha, \beta) = \sum_{i=1}^{n} | \alpha_i - \beta_i |$$

Cette distance a toutes les propriétés d'une métrique. Elle donne le nombre de positions où les deux suites α et β diffèrent l'une de l'autre. Dans le langage de la théorie des communications, si α est le message transmis et β le message reçu, $\delta(\alpha, \beta)$ est alors le nombre d'erreurs de transmission.

Si l'on définit maintenant une opération $\oplus$ ("addition") sur C_n par la relation :

$$\alpha \oplus \beta = (\alpha_1 \oplus \beta_1, \alpha_2 \oplus \beta_2, \ldots, \alpha_n \oplus \beta_n)$$

où, pour les nombres α_i et β_i, le signe $\oplus$ représente l'addition modulo 2, on voit que :

(i) l'opération $\oplus$ est associative et commutative,

(ii) Si $\alpha \in C_n$ et $\beta \in C_n$, alors

$$\alpha \oplus \beta \in C_n,$$

(iii) il existe un élément neutre ou zéro

$$\emptyset = (0, 0, \ldots, 0),$$

tel que $$\alpha \oplus \emptyset = \emptyset \oplus \alpha = \alpha ,$$

(iv) tout élément $\alpha \in C_n$ est son propre inverse, c'est-à-dire,

$$\alpha \oplus \alpha = \emptyset$$

pour tout $\alpha \in C_n$.

Ainsi, par rapport à l'opération $\oplus$, C_n est un groupe abélien fini d'ordre 2^n et de type (1, 1, ... , 1). On a évidemment :

$$\delta(\alpha, \beta) = \| \alpha \oplus \beta \|$$

On appelle code à distance d tout sous-ensemble de C_n tel que si α, β ($\alpha \neq \beta$) appartiennent à ce sous-ensemble on ait :

$$\delta(\alpha, \beta) = \| \alpha \oplus \beta \| \geqslant d.$$

L'importance de tels sous-ensembles pour la théorie des communications est évidente. Si les messages transmis font partie d'un code à distance $d = 2k + 1$, on peut alors rectifier jusqu'à k erreurs de transmission. Il suffit d'entourer chaque point du code par une "sphère" de rayon k. Si le nombre d'erreurs de transmission ne dépasse pas k, le message reçu se trouvera dans la sphère qui entoure le message transmis et l'identification de celui-ci se fera sans erreur.

Un code φ à distance d est appelé un code optimal si pour tout élément :

$$\alpha \in C_n, \alpha \notin \varphi$$

il existe au moins un élément $\bar{\alpha} \in \varphi$, tel que

$$\| \alpha \oplus \bar{\alpha} \| < d.$$

C'est-à-dire qu'une fois trouvé un code optimal, il est impossible d'y ajouter de nouveaux points sans détruire la propriété de distance minima. Nous désignerons les codes optimaux de C_n à distance d par $M(n, d)$.

Etant donnés n et d, il existe plusieurs codes optimaux et il n'est

pas vrai que deux codes optimaux ont le même nombre d'éléments. Par exemple, pour n = 6 et d = 3 nous avons les trois codes optimaux suivants ayant respectivement 4, 6 et 8 éléments.

1)	2)	3)
00 00 00	00 00 00	00 00 00
01 01 01	01 01 01	01 01 01
10 10 10	10 01 10	10 01 10
11 11 11	11 10 00	11 00 11
	00 10 11	00 10 11
	11 11 11	01 11 10
		10 11 01
		11 10 00

Nous désignerons par $[M(n,d)]$ le nombre d'éléments contenus dans M, et nous dirons que M_1 est plus grand que M_2 si :

$$[M_1(n,d)] > [M_2(n,d)].$$

Le problème principal du codage binaire est la recherche du code optimal le plus grand. On ne connait jusqu'à présent aucune méthode générale pour construire de tels codes, ni aucune expression générale pour la valeur de $[M(n,d)]$. Laemmel (1952) a donné une table fournissant, pour n = 1, 2, 3, ..., 17 et d = 1, 2, ..., 13, le nombre d'éléments du code optimal le plus grand connu jusqu'à présent.

Hamming (1950), qui pour la première fois avait posé de cette façon le problème du codage binaire, n'a considéré que les codes qu'il appelait systématiques. Un code systématique est un code où parmi les n positions on en choisit un certain nombre m appelés positions d'information, les n-m positions qui restent étant les positions de contrôle ou de vérification. Les symboles dans les positions d'information sont choisis arbitrairement tandis que ceux qui figurent dans les positions de contrôle sont des fonctions linéaires déterminées des premiers. Plus tard Slepian (1956) dans son étude sur les codes qui sont des sous-groupes de C_n a démontré que tout code systématique est un sous-groupe et qu'inversement tout code sous-groupe peut être considéré comme un code systématique. Les codes optimaux qui ne seraient pas des sous-groupes étaient connus de Hamming. Il les appelait les codes non-systématiques - et il avait conjecturé que le code optimal le plus grand est toujours un code systématique, c'est-à-dire un sous-groupe. Ceci pourtant n'est pas vrai car pour n = 9, d = 5, le plus grand code contient 6 points et n'est donc pas un sous-groupe.

D'autre part Reed (1953) se servant des méthodes utilisées par Muller (1953) pour la recherche des fonctions booléennes a donné une méthode pour construire des codes à distance donnée. Sa méthode ne s'applique qu'au cas où :

$$n = 2^m, \quad d = 2^r$$

m et r étant des nombres entiers positifs. Les codes ainsi construits sont aussi des sous-groupes, mais on ne sait pas s'ils sont toujours optimaux.

Nous allons d'abord étudier quelques propriétés générales des codes optimaux. Le théorème suivant est dû à Hamming (1950).

THEOREME 1 -

Pour tout code optimal M(n, 2k) il existe un code optimal M(n-1,2k-1) tel que :

$$[M(n, 2k)] = [M(n-1, 2k-1)]$$

Hamming a aussi donné la borne supérieure

$$[M(n, 2k)] \leqslant \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k}}$$

et Gilbert (1952) a trouvé la borne inférieure

$$M(n, 2k+1) \geqslant \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{2k}}$$

(Pour d'autres relations du même genre voir Laemmel (1952)).

Soit maintenant φ un code (non nécessairement optimal) à distance d. Alors, pour tout $\alpha \in C_n$, l'ensemble des points :

$$\alpha \oplus \beta \ , \ \beta \in \varphi$$

est aussi un code à distance d.

Car : $\| (\alpha \oplus \beta_i) \oplus (\alpha \oplus \beta_j) \| = \| \beta_i \oplus \beta_j \| \geqslant d.$

Nous avons en fait le théorème suivant.

THEOREME 2 -

Si φ est un code optimal à distance d, alors pour tout $\alpha \in C_n$, l'ensemble $\{ \alpha \oplus \varphi \}$ est, lui aussi, un code optimal d et inversement.

Soient

$$\beta_1, \beta_2, \ldots, \beta_m$$

les éléments du code φ. Si φ est un code optimal et que l'ensemble $\{\alpha \oplus \varphi\}$ c'est-à-dire, l'ensemble :

$$(\alpha \oplus \beta_1, \alpha \oplus \beta_2, \ldots, \alpha \oplus \beta_m)$$

ne l'est pas, nous pouvons trouver un élément $\gamma \in C_n$ tel que :

$$\begin{matrix} \gamma \neq \alpha \oplus \beta_i \\ \| \gamma \oplus (\alpha \oplus \beta_i) \| \geqslant d \end{matrix} \qquad i = 1, 2, \ldots, m.$$

De là on voit que l'élément $\alpha \oplus \gamma$ n'appartient pas à φ et que sa distance de tout élément de φ est supérieure ou égale à d. C'est-à-dire que φ n'est pas non plus un code optimal. L'inverse se démontre de même façon.

Considérons maintenant un code optimal M(n, d) et désignons par

$$a_1, a_2, \ldots, a_m$$

ses éléments. Ainsi on a $[M(n, d)] = m$.

Si l'on désigne par A_i l'ensemble des points dont la distance du point a_i est inférieure à d, et par $\overline{M}$ l'ensemble complémentaire de M par rapport à l'espace C_n, on a :

$$A_i \subset \overline{M} \qquad \text{et} \qquad \bigcup_{i=1}^{m} A_i = \overline{M}$$

La première propriété est évidente. Pour la seconde, si elle n'était pas vraie, il existerait un élément dans $\overline{M}$ dont la distance à tout point de M serait supérieure ou égale à d, ce qui est impossible d'après l'optimalité du code M. Si l'on désigne, pour tout sous-ensemble E de C_n, l'ordre (c'est-à-dire le nombre d'éléments) du plus grand code optimal à distance d contenu dans E par $[E]_d$ on a le théorème suivant.

THEOREME 3 -

Pour qu'un code optimal M(n, d) soit le code optimal le plus grand il faut, et il suffit, que l'on ait :

$$[\overline{M} - \bigcup_{a_i \in M^*} A_i]_d \leqslant [M - M^*]$$

pour tout sous-ensemble $M^* \subset M$.

Le théorème, dont la démonstration est évidente, doit être considéré plutôt comme une définition du code optimal le plus grand, laquelle définition pourrait servir comme point de départ pour trouver d'autres résultats de plus grande utilité.

Les codes qui sont des sous-groupes.

Les codes optimaux qui sont aussi des sous-groupes de C_n jouent un rôle très important. En effet la plupart des codes étudiés jusqu'à présent étaient effectivement des sous-groupes. L'importance et l'utilité de tels codes sont montrés par les considérations suivantes. Nous avons tout d'abord deux lemmes.

Lemme 1 :

Soit φ un sous-groupe de C_n et soit :

$$d = \inf_{\substack{\alpha \in \varphi \\ \alpha \neq \emptyset}} \| \alpha \|$$

Alors φ est un code à distance d. Car, si α_1 , α_2 sont deux éléments différents de φ, on a $\alpha_1 \oplus \alpha_2 \in \varphi$

Par conséquent :

$$\| \alpha_1 \oplus \alpha_2 \| \geqslant d.$$

Lemme 2 :

Soit φ un sous-groupe de C_n à distance d, et soit α un élément de C_n, tel que $\alpha \notin \varphi$ et que $\| \alpha \oplus \beta \| \geqslant d$, pour tout élément $\beta \in \varphi$.

Alors l'ensemble $\varphi_1 = \{ \alpha \oplus \varphi \} \cup \varphi$ est, lui aussi, un sous-groupe à distance d.

Soient :

$$\emptyset, \beta_1 , \ldots , \beta_m$$

les éléments de φ. Alors les éléments de φ_1 sont :

$$\emptyset, \beta_1 , \ldots , \beta_m$$

$$\alpha , \alpha \oplus \beta_1 , \ldots , \alpha \oplus \beta_m$$

Ces éléments sont tous différents et on voit immédiatement que la somme de deux éléments de φ_1 appartient à φ_1 et que la distance entre deux éléments différents quelconques de φ_1 est supérieure ou égale à d. Le lemme est donc démontré. De plus nous avons :

$$[\varphi_1] = 2\ [\varphi]$$

Nous désignerons, pour tout sous-groupe φ de C_n, le groupe quo-

tient par $C_n \mid \varphi$. Dans tout complexe φ_i du groupe quotient on peut choisir un élément représentatif α_i tel que tout élément de φ_i peut être représenté comme $\alpha_i \oplus \beta$ où β est l'un des éléments de φ. Tout complexe du groupe quotient contient le même nombre d'éléments que le sous-groupe .

THEOREME 4 -

Le plus grand sous-groupe de C_n dont tous les éléments, sauf l'élément neutre, sont de norme supérieure ou égale à d est un code optimal à distance d.

Soit G le sous-groupe en question et désignons par G_α, G_β, G_γ, ... les complexes du groupe quotient $C_n \mid G$, où α, β, γ, ... désignent les éléments représentatifs de ces complexes. G est un sous-groupe à distance d (cf. lemme 1). Supposons que G ne soit pas optimal. Il existe alors un élément de C_n n'appartenant pas à G, soit l'élément α, tel que

$$\| \alpha \oplus g_i \| \geqslant d$$

pour tout élément $g_i \in G$.

On voit alors que (cf. lemme 2) l'ensemble $G_\alpha \cup G$ est, lui aussi, un sous-groupe dont tout élément sauf l'élément neutre est de norme supérieure ou égale à d. Mais ceci est contraire à l'hypothèse que G est le plus grand sous-groupe de ce genre. Le théorème est ainsi démontré.

Il existe, à part G, d'autres sous-groupes ayant la propriété optimale. Nous en avons déjà vu un exemple pour le cas où n = 6, d = 3. Le théorème suivant donne une condition nécessaire et suffisante pour qu'un sous-groupe à distance d soit aussi optimal.

THEOREME 5 -

Une condition nécessaire et suffisante pour qu'un sous-groupe φ à distance d soit un code optimal est qu'il existe au moins un élément de norme inférieure à d dans tout complexe du groupe quotient $C_n \mid \varphi$.

Soient :

$$\alpha_0 = \emptyset, \alpha_1, \alpha_2, \ldots, \alpha_m$$

les éléments de φ et soient $\varphi_1, \varphi_2, \ldots, \varphi_r$

les complexes du groupe quotient $C_n \mid \varphi$. Désignons par β_i l'élément représentatif de φ_i. Tout élément de φ_i est de la forme :

$$\beta_i \oplus \alpha_j \ , \ j = 0, 1, \ldots, m \ ,$$

Si le sous-groupe φ est un code optimal, il existe, par définition, pour tout élément β_i au moins un élément $\alpha_j \in \varphi$, tel que :

$$\| \beta_i \oplus \alpha_j \| < d$$

et la condition est nécessaire.

Si l'on suppose, au contraire, que tout complexe contient au moins un élément de norme inférieure à d, on voit que pour tout élément de C_n n'appartenant pas à φ (c'est-à-dire appartenant à l'un des complexes φ_i) correspond au moins un élément de φ tel que la norme de la somme de ces deux éléments est inférieure à d. Ce qui démontre que φ est un code optimal et que la condition est suffisante.

A partir de ces considérations on peut maintenant donner une méthode simple pour construire des codes optimaux qui, de plus, aboutit toujours à des sous-groupes. Soit d la distance. Prenons l'élément neutre $\emptyset$ choisissons un élément quelconque $\alpha \in C_n$ tel que $\| \alpha \| \geq d$.

Alors l'ensemble $\{ \emptyset, \alpha \}$ est un sous-groupe à distance d. S'il n'est pas optimal il existe au moins un élément, soit β, tel que :

$$\| \beta \| \geq d, \quad \| \alpha \oplus \beta \| \geq d.$$

Alors l'ensemble $\{ \emptyset, \alpha, \beta, \alpha \oplus \beta \}$ est encore un sous-groupe à distance d. S'il n'est pas optimal, il existe un élément, soit γ, dont la distance à chacun de ces quatre points est supérieure ou égale à d. Alors l'ensemble des points :

$$\emptyset, \alpha, \beta, \alpha \oplus \beta, \gamma, \alpha \oplus \gamma, \beta \oplus \gamma, \alpha \oplus \beta \oplus \gamma$$

constitue encore un sous-groupe à distance d. Ou bien il est optimal, ou bien s'il ne l'est pas, on peut continuer le raisonnement ci-dessus et obtenir un autre sous-groupe (de 16 éléments) à distance d et ainsi de suite.

Soit φ un sous-groupe optimal à distance d et soient $\varphi_\alpha, \varphi_\beta, \varphi_\gamma, \ldots$ les complexes du groupe quotient $C_n | \varphi$. $\alpha, \beta, \gamma, \ldots$ sont ici les éléments représentatifs de $\varphi_\alpha, \varphi_\beta, \varphi_\gamma, \ldots$. Nous désignerons par $\varphi_{\alpha \oplus \beta}$ le complexe résultant de l'addition de complexes φ_α et φ_β.

Soit m_α le nombre d'éléments de φ_α de norme inférieure à d. On a alors les propriétés suivantes.

(i) $m_\alpha > 0, \; m_\beta > 0, \; \ldots$

$$m_\alpha + m_\beta + \ldots = \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{d-1}$$

(ii) A tout élément α de φ_α correspond exactement m_α éléments de φ dont la distance à α est inférieure à d.

(iii) A tout élément $\alpha \in \varphi_\alpha$ correspond exactement $m_{\alpha\oplus\beta}$ éléments de φ_β dont la distance à α est inférieure à d.

(iv) Si l'on désigne par $\varphi_{\beta(\alpha)}$ l'ensemble des points de φ_β dont la distance à $\alpha \in \varphi_\alpha$ est inférieure à d, alors :

$$\bigcup_{\alpha\in\phi_\alpha} \varphi_\beta(\alpha) = \varphi_\beta$$

Ces propriétés découlent des propriétés bien connues du groupe quotient et du fait que φ, et donc φ_α, φ_β, ... aussi, sont des codes optimaux (cf. théorème 2). En les utilisant on a le théorème suivant.

THEOREME 5[a] -

Soit φ un sous-groupe optimal à distance d et soient φ_α, φ_β, φ_γ trois complexes du groupe quotient $C_n \mid \varphi$ tels que:

$$m_{\alpha\oplus\gamma} = m_{\beta\oplus\gamma} = 1 .$$

s'il existe des éléments :

$$\alpha \in \varphi_\alpha,\ \beta \in \varphi_\beta,\ \gamma \in \varepsilon\ \varphi_\gamma$$

tels que :

$$\| \alpha \oplus \beta \| \geqslant d, \quad \| \alpha \oplus \gamma \| < d, \quad \| \beta \oplus \gamma \| < d$$

alors il existe un code à distance d d'ordre supérieur à $[\varphi]$.

A tout élément de φ_α et de φ_β correspond un seul élément de φ_γ dont la distance à ces éléments est inférieure à d. Les conditions du théorème montrent qu'aux deux éléments α et β correspond le même élément $\gamma \in \varphi_\gamma$. Ainsi dans l'ensemble optimal φ_γ on peut remplacer l'élément γ par les deux éléments α et β. L'ensemble ainsi obtenu est un ensemble à distance d et d'ordre supérieur à $[\varphi_\gamma] = [\varphi]$. Le théorème est donc démontré.

Exemple : Prenons le cas n = 6, d = 3. Le sous-groupe :

00 00 00
01 01 01
10 10 10
11 11 11

est un code optimal. Le groupe quotient contient 15 complexes dont les éléments représentatifs sont :

1) 00 00 01	6) 10 00 00	11) 10 01 10
2) 00 00 10	7) 00 01 11	12) 01 01 10
3) 00 01 00	8) 00 10 11	13) 01 10 10
4) 00 10 00	9) 00 11 01	14) 01 11 00
5) 01 00 00	10) 00 11 10	15) 10 11 00

Si l'on prend :

$$\varphi_\alpha = \varphi_{14} \quad , \quad \varphi_\beta = \varphi_6 \quad , \quad \varphi_\gamma = \varphi_3$$

on a :

$$m_{\alpha\oplus\gamma} = m_9 = 1$$

$$m_{\beta\oplus\gamma} = m_{10} = 1$$

On peut également choisir trois éléments α, β , γ

$$\alpha\in\varphi_{14} \quad : 01\ 11\ 00$$

$$\beta\in\varphi_6 \quad : 10\ 00\ 00$$

$$\gamma\in\varphi_3 \quad : 00\ 01\ 00$$

et on a :

$$\|\alpha\oplus\beta\| = 4 \ , \qquad \|\alpha\oplus\gamma\| = 2 \ , \qquad \|\beta\oplus\gamma\| = 2,$$

et le code optimal n'est pas le plus grand. En effet nous avons déjà vu qu'il existe un sous-groupe à distance 3 ayant 8 éléments.

Les deux théorèmes suivants donnent des conditions suffisantes pour qu'un sous-groupe optimal soit aussi le plus grand code optimal.

THEOREME 6 -

Soit φ un sous-groupe optimal à distance d et soient :

$$\varphi_i \ , \ i = 1, 2, \ldots , r$$

les complexes du groupe quotient. S'il existe des éléments représentifs $\alpha_i \in \varphi_i$,

tels que :

$$\left.\begin{array}{r} \| \alpha_i \| < d \\ \| \alpha_i \oplus \alpha_j \| < d \end{array}\right\} \quad \begin{array}{c} i, j = 1, 2, \ldots, r \\ i \neq j \end{array}$$

alors, φ est le code optimal le plus grand. Désignons par

$$g_0 = \emptyset, g_1, g_2, \ldots, g_s$$

les éléments de φ. Tout élément d'un complexe φ_i s'écrit :

$$\alpha_i \oplus g_j, j = 0, 1, \ldots, s.$$

Soit M(n, d) un code optimal quelconque et soient :

$$m_1, m_2, \ldots, m_t$$

ses éléments. Nous allons maintenant établir une correspondance biunivoque entre les éléments de M et ceux de φ.

Supposons qu'un élément $m_k \in M$ appartient à φ_i, soit $m_k = \alpha_i \oplus g_1$. Dans ce cas on associe l'élément g_1 à m_k. Si l'élément $m_k \in M$ appartient à φ, soit $m_k = g_k$ on lui associe l'élément g_k.

On voit immédiatement que c'est une correspondance biunivoque où à chaque élément de M correspond un et un seul élément de φ et à deux éléments différents de M correspondent deux éléments différents de φ. Car si deux éléments de M appartiennent au même complexe φ_i deux éléments différents de φ correspondent à eux. Si par contre deux éléments m_a et m_b de M appartiennent à deux complexes différents, soient à φ_a et φ_b, on a :

$$m_a = \alpha_a \oplus g_i$$

$$m_b = \alpha_b \oplus g_j$$

et on doit avoir $g_i \neq g_j$, sinon on aurait $\| m_a \oplus m_b \| = \| \alpha_a \oplus \alpha_b \| < d$. Le même raisonnement s'applique au cas où un élément de M appartient à un complexe φ_i et l'autre au sous-groupe φ. Ce qui démontre le théorème.

THEOREME 7 -

Soit φ un sous-groupe optimal à distance d d'ordre 2^{μ} (μ entier positif) et soient φ_i ($i = 1, 2, \ldots, r, r = 2^{n-\mu} - 1$) les complexes du groupe quotient. Si $\mu < (n/2)$, et s'il existe des éléments représentatifs $\alpha_i \in \varphi_i$ tels que :

$$\| \alpha_i \oplus \alpha_j \| < d \; ; \; i, j = 1, 2, \ldots, r, \qquad i \neq j$$

alors, φ est le code optimal le plus grand.

Soit M(n, d) un code optimal quelconque. Si M ne contient que des éléments appartenant aux complexes φ_i, c'est-à-dire si son intersection (au sens de la théorie des ensembles) avec φ est vide, on voit que d'après les conditions ci-dessus énoncées la correspondance établie dans le théorème précédent associe à chaque élément de M un et un seul élément de φ et qu'à deux éléments différents de M correspondent deux éléments différents de φ. Dans ce cas, donc, l'ordre de M est au plus égal à l'ordre de φ.

Soit maintenant M'(n, d) un code optimal ayant des éléments communs avec le sous-groupe φ. Comme $\mu < (n/2)$, le nombre r de complexes φ_i est supérieur à 2^{μ}. Il existe donc au moins un complexe, soit φ_k, dont l'intersection avec M' est vide. Prenons un élément quelconque $\alpha_k \in \varphi_k$ et considérons l'ensemble :

$$M'' = \{ \alpha \oplus M' \} .$$

D'après le théorème 2, M'' est aussi un code optimal du même ordre que M'. Mais M'' n'a aucun élément en commun avec φ. Par conséquent l'ordre de M'', et donc celui de M' aussi, est au plus égal à l'ordre de φ. Ceci achève la démonstration du théorème.

Nous allons maintenant étudier deux cas particuliers des codes optimaux qui sont des sous-groupes.

I - <u>$n = 2^m - 1$, $d = 3$ (m entier positif)</u> -

Il y a $(2^m - 1)$ éléments de norme 1 et d'après un théorème de Zaremba (1952, théorème 1) il existe un sous-groupe φ d'ordre 2^{n-m} tel que les éléments de norme 1 peuvent être pris comme éléments représentatifs des $(2^m - 1)$ complexes φ_i, du groupe quotient $C_n \mid \varphi$. On voit facilement que tout élément de φ sauf l'élément neutre est de norme supérieure ou égale à 3. Ainsi φ est un code à distance 3 (cf. lemme 1). D'après le théorème 5, φ est aussi optimal. Il est intéressant de noter que dans ce cas le code optimal φ atteint la borne supérieure de Hamming car :

$$[\varphi] = 2^{n-m} = \frac{2^n}{1 + n}$$

II - <u>$n = \frac{2}{3}(2^{2r} - 1)$, $d = 3$ (r entier positif)</u> -

Un autre théorème de Zaremba (1952, prop. 2) montre qu'il existe

un sous-groupe φ d'ordre 2^{n-2r} tel que tout élément de φ, à l'exception de l'élément neutre, est de norme supérieure ou égale à 3 et que tout complexe du groupe quotient contient au moins un élément de norme inférieure à 3. Ce qui démontre que le sous-groupe φ ainsi trouvé est un code optimal à distance 3.

Les codes qui ne sont pas des sous-groupes.

Considérons maintenant les codes optimaux qui ne sont pas des sous-groupes. Notons tout d'abord que tout code sous-groupe engendre automatiquement des codes qui ne sont pas des sous-groupes, à savoir les complexes appartenant au groupe quotient. On sait, d'après le théorème 2, que si le sous-groupe en question est un code optimal, tout complexe appartenant au groupe quotient est, lui aussi, un code optimal avec la même distance que le sous-groupe. D'ailleurs tout complexe appartenant au groupe quotient a le même nombre d'éléments que le sous-groupe. Aussi ce ne sont pas ces complexes qui nous intéressent, car la question la plus importante est de savoir sous quelles conditions le code optimal le plus grand n'est pas un sous-groupe. Qu'il existe de tels codes est bien connu et nous en avons déjà parlé. Les deux théorèmes suivants donnent des conditions nécessaires pour qu'un code optimal qui n'est pas un sous-groupe soit le plus grand.

Nous supposerons que le code optimal en question contient toujours l'élément neutre $\emptyset$. Ceci n'est pas une condition restrictive car si l'élément neutre ne fait pas partie du code on peut toujours transformer celui-ci de telle sorte qu'on obtienne un autre code du même ordre et contenant l'élément neutre. Il suffit de prendre un élément quelconque α du code M et de considérer, au lieu de M, le code transformé :

$$M' = \{\alpha \oplus M\} .$$

(cf. théorème 2).

THEOREME 8 -

Soit M(n, d) un code optimal d'ordre m contenant l'élément neutre $\emptyset$. Si M n'est pas un sous-groupe, soit r l'ordre du plus grand sous-groupe contenu dans M. Alors une condition nécessaire pour que M soit le plus grand code optimal est que :

$$r < (m / 2) .$$

Si φ désigne le plus grand sous-groupe contenu dans M, et α un élément quelconque de M - φ (il existe au moins un tel élément), l'ensemble :

$$\varphi_1 = \{ \alpha \oplus \varphi \} \cup \varphi$$

est aussi un code à distance d (cf. lemme 2). Comme $[\varphi_1] = 2 [\varphi] = 2r$ la nécessité de la condition est évidente.

Avant de passer au théorème suivant nous introduisons la définition d'un ensemble fermé sous l'addition des éléments différents. Nous dirons qu'un ensemble $E \subset C_n$ est fermé sous l'addition des éléments différents si pour tout couple d'éléments :

$$\alpha, \beta \in E, \qquad \alpha \neq \beta \quad ;$$

leur somme $\alpha \oplus \beta$ appartient, elle aussi, à l'ensemble E. Remarquons qu'un ensemble fermé sous l'addition des éléments différents devient un sous-groupe si l'on y ajoute l'élément neutre $\emptyset$ et qu'inversement si φ est un sous-groupe l'ensemble $\{ \varphi - \emptyset \}$ est un ensemble fermé sous l'addition des éléments différents.

THEOREME 9 -

Soit M(n, d) un code optimal d'ordre m contenant l'élément neutre. Si M n'est pas un sous-groupe, soit r l'ordre du plus grand sous-groupe φ contenu dans M, et s l'ordre du plus grand ensemble E fermé sous l'addition des éléments différents, contenu dans $M - \varphi$. Alors, une condition nécessaire pour que M soit le plus grand code optimal est que :

$$r(s+1) < m.$$

Désignons par $g_0 = \emptyset$, $g_1, g_2, \ldots, g_{r-1}$ les éléments de φ, et par $h_1, h_2, \ldots, h_s$ les éléments de E. E et φ étant des sous-ensembles de M, on a évidemment :

$$\| g_i \oplus h_j \| \geqslant d.$$

Considérons maintenant l'ensemble :

$$\varphi \cup \{ h_1 \oplus \varphi \} \cup \{ h_2 \oplus \varphi \} \ldots \cup \{ h_s \oplus \varphi \}$$

Cet ensemble est d'ordre r(s + 1). Tout couple d'éléments de cet ensemble appartient à l'une des trois catégories suivantes :

(i) (g_i, g_j)

(ii) $(g_i, h_j \oplus g_k)$

(iii) $(h_i \oplus g_j, h_k \oplus g_l)$

et nous avons :

$$\| g_i \oplus g_j \| \geqslant d$$

$$\| g_i \oplus (h_j \oplus g_k) \| = \| h_j \oplus g_1 \| \geqslant d$$

$$\| (h_i \oplus g_j \oplus (h_k \oplus g_1) \| = \| (h_i \oplus h_k) \oplus (g_j \oplus g_1) \| = \| h_a \oplus g_b \| \geqslant d.$$

On voit que cet ensemble d'ordre $r(s + 1)$ satisfait à la condition de distance minima. Ce qui démontre que la condition est nécessaire.

Le nombre d'éléments d'un code optimal -

Le problème général de trouver le nombre d'éléments contenus dans un code optimal le plus grand n'a pas encore trouvé de solution. Dans l'absence d'une solution générale la recherche des bornes supérieures devient important surtout parce que la borne supérieure de Hamming (1950) donne des valeurs trop grandes. Nous donnons ci-dessous deux résultats qui sont plus simples et dont le second donne les valeurs beaucoup plus petites que celles de Hamming.

THEOREME 10 -

$$[M(n, d)] \leqslant 2^{n-d+1}$$

Nous supposerons toujours que le code $M(n, d)$ contient l'élément neutre $\emptyset$. Soient :

$$\alpha_0 = \emptyset, \alpha_1, \alpha_2, \ldots, \alpha_r. \qquad r = 2^{d-1} - 1$$

les éléments du sous-groupe φ de C_n obtenu en ajoutant $n-d+1$ zéros à tous les éléments de C_{d-1}. Les ensembles :

$$\{ M \oplus \alpha_i \} \qquad i = 0, 1, \ldots, r$$

sont disjoints et on a donc :

$$[M(n, d)] \cdot 2^{d-1} \leqslant 2^n$$

ce qui nous donne le résultat énoncé. Signalons que Komamiya (1954) a obtenu le même résultat en utilisant un raisonnement plus compliqué.

THEOREME 11 -

Si la distance d est un nombre impair et si $2d + 1 > n$, on a :

$$[M(n, d)] \leqslant \frac{2d + 2}{2d + 1 - n}$$

Désignons les éléments de M(n, d) par

$$\alpha_1, \alpha_2, \ldots, \alpha_m \; ; \qquad m = [\, M(n,d) \,]$$

et formons la matrice à m lignes et n colonnes dont la j-ième ligne est l'élément α_j. Si l'on désigne par k_i (i = 1, 2, ... , n) la somme de la i-ième colonne on obtient :

$$n.\ \text{variance}\ (k_i) = mA - \frac{A^2}{n} - \sum_{\alpha_j \neq \alpha_k} \delta(\alpha_j, \alpha_k)$$

où on a :

$$A = \sum_i k_i = \sum_j \| \alpha_j \|$$

Ce résultat est valable non seulement pour les codes optimaux mais pour tout sous-ensemble de C_n (cf. Schutzenberger (1953)).

Cela nous donne :

$$\sum_{j \neq k} \delta(\alpha_j, \alpha_k) \leqslant mA - \frac{A^2}{n}$$

La valeur de A est comprise entre 0 et mn et la quantité $mA - \frac{A^2}{n}$ atteint son maximum pour $A = \frac{mn}{2}$. On a donc :

$$\sum_{j \neq k} \delta(\alpha_j, \alpha_k) \leqslant \frac{m^2 n}{4}$$

Tous les $\delta(\alpha_j, \alpha_k)$ étant supérieurs ou égaux à d, on obtient une première inégalité valable pour toute la valeur de d :

$$\left[\frac{m(m-1)}{2} \right] d \leqslant \frac{m^2 n}{4}$$

c'est-à-dire :

$$m \leqslant \frac{2d}{2d - n}$$

à condition que l'on ait 2d > n.

Supposons que d soit un nombre impair et que des m éléments de M(n, d) r soient de norme impaire et s de norme paire (r + s = n). La distance entre deux éléments de norme paire ainsi qu'entre deux éléments de norme impaire est un nombre pair tandis que la distance entre un élément de norme paire et un élément de norme impaire est un nombre impair.

Comme d est un nombre impair si la distance entre deux éléments est un nombre pair elle est au moins égale à d + 1. Nous avons donc :

$$\left\{ \frac{r\,(r - 1)}{2} + \frac{s\,(s - 1)}{2} \right\} (d + 1) + rsd \leqslant \frac{m^2 n}{4}$$

ce qui donne finalement :

$$m \leqslant \frac{2d + 2}{2d + 1 - n}$$

à condition que l'on ait $2d + 1 > n$.

En titre de comparaison nous donnons ci-dessous (Table I) les valeurs de la borne supérieure de Hamming et celle du théorème 11. La première valeur est celle fournie par le résultat de Hamming et la seconde celle du théorème 11. Nous avons ajouté entre parenthèses le nombre d'éléments du code optimal le plus grand effectivement construit (d'après Laemmel (1952)). Il est intéressant de remarquer que dans plusieurs cas (eg. n = 9, d = 5) notre résultat permet de démontrer que le code construit est aussi le plus grand possible.

- TABLE I -

n \ d	3	5	7	9	11
5	5,3 4(4)				
6	9,1 8(8)				
7		4,4 3(2)			
8		6,9 4(4)			
9		11,1 6(6)	3,9 2,6(2)		
10		18,3 12(12)	5,8 3,2(2)		
11			8,8 4(4)		
12			13,7 5,3(4)	5,2 2,9(2)	
13			21,7 8(8)	7,5 3,3(2)	
14			34,9 16(16)	11,1 4(4)	4,7 2,7(2)
15				16,9 5(4)	6,6 3(2)
16				26,0 6,6	9,5 3,4(2)
17				40,8 10	13,9 4(4)

CHAPITRE III

LE THÉORÈME FONDAMENTAL : CAS GÉNÉRAL

DEFINITIONS ET THEOREMES PRELIMINAIRES :

Soit X un ensemble d'éléments x de nature quelconque. Nous appellerons x un point de l'espace X. Soit $\mathscr{X}$ une famille de sous-ensembles de X telle que :

(i) $E \in \mathscr{X}$, $F \in \mathscr{X}$ entraîne $E \cup F \in \mathscr{X}$ et $E \cap F \in \mathscr{X}$

(ii) $E \in \mathscr{X}$ entraîne $\bar{E} \in \mathscr{X}$, où $\bar{E}$ est l'ensemble complémentaire de E par rapport à X ;

$\mathscr{X}$ est alors un corps. Si $\mathscr{X}$ est tel que l'union de toute suite dénombrable $\{E_i\}$ d'ensembles de $\mathscr{X}$ appartient à $\mathscr{X}$, alors $\mathscr{X}$ est un corps borélien (ou σ - corps). Un espace X sur lequel est défini un corps borélien $\mathscr{X}$ de sous-ensembles de X est appelé un espace mesurable, et nous le désignerons par $(X, \mathscr{X})$. On appelle ensemble mesurable tout sous-ensemble de X appartenant à $\mathscr{X}$.

Une fonction d'ensemble μ définie sur $\mathscr{X}$ est une mesure si elle est non-négative et complètement additive ; μ est une mesure finie si $\mu(X) < +\infty$; μ est une mesure σ - finie s'il existe une suite dénombrable ou finie d'ensembles mesurables E_i telle que $\bigcup_i E_i = X$, et que $\mu(E_i) < +\infty$ pour tout i. La mesure μ est une mesure de probabilité si $\mu(X) = 1$.

Soient μ, ν deux mesures définies sur un même espace mesurable $(X, \mathscr{X})$. Si pour tout ensemble $E \in \mathscr{X}$ pour lequel $\mu(E) = 0$, on a $\nu(E) = 0$, on dit que la mesure ν est absolument continue par rapport à μ, et on écrit :

$$\nu << \mu$$

Si l'on a à la fois $\nu << \mu$ et $\mu << \nu$, alors on dit que μ et ν sont équivalentes, et on écrit :

$$\mu \equiv \nu$$

Si pour μ et ν, il existe deux ensembles disjoints A et B tels que $A \cup B = X$ que pour tout ensemble $E \in \mathfrak{X}$ on ait $(A \cap E) \in \mathfrak{X}$ et $(B \cap E) \in \mathfrak{X}$, et que :

$$\mu(A \cap E) = \nu(B \cap E) = 0,$$

alors, on dit que μ et ν sont singulières l'une par rapport à l'autre, et on écrit :

$$\mu \perp \nu .$$

Une fonction à valeurs réelles $f(x)$ définie sur l'espace mesurable $(X, \mathfrak{X})$ est une fonction mesurable $(\mathfrak{X})$ si pour tout nombre réel c, l'ensemble :

$$\{ x : f(x) < c \}$$

appartient à $\mathfrak{X}$. On a le théorème suivant :

THEOREME DE RADON-NIKODYM :

Si μ et ν sont deux mesures σ - finies sur l'espace mesurable $(X, \mathfrak{X})$ telles que $\nu << \mu$, alors, il existe une fonction $f(x)$ mesurable $(\mathfrak{X})$, telle que :

$$0 < f(x) < +\infty$$

et que tout ensemble $E \in \mathfrak{X}$

$$\nu(E) = \int_E f(x)\, d\mu(x).$$

La fonction $f(x)$ est unique dans ce sens que s'il existe une autre fonction $g(x)$ ayant les mêmes propriétés que $f(x)$, on a :

$$\mu \{ x : f(x) \neq g(x) \} = 0.$$

On écrira :

$$d\nu(x) = f(x)\, d\mu(x) \quad \text{et aussi :} \quad f(x) = d\nu / d\mu.$$

Soient $(X, \mathfrak{X})$ et $(Y, \mathcal{Y})$ deux espaces mesurables. On appelle espace produit de X et de Y l'ensemble de couples ordonnés (x, y) où $x \in X$ et $y \in Y$. Nous le noterons par $X \otimes Y$. De même, pour tout ensemble $E \in \mathfrak{X}$ et $F \in \mathcal{Y}$, nous désignerons par $E \otimes F$ l'ensemble, appelé rectangle mesurable, des points (x, y) tels que $x \in E$, $y \in F$. Le plus petit corps borélien sur $X \otimes Y$ qui contient tous les rectangles mesurables sera désigné par $\mathfrak{X} \otimes \mathcal{Y}$. On définit de la même façon l'espace produit d'un nombre fini quelconque d'espaces mesurables.

On sait que la famille $\mathcal{R}$ de sous-ensembles de $X \otimes Y$ qui, à part les rectangles mesurables, contient toute réunion d'un nombre fini de ceux-ci est un corps. Le corps borélien $\mathcal{X} \otimes \mathcal{Y}$ peut aussi être considéré comme le plus petit corps borélien qui contient tous les ensembles du corps $\mathcal{R}$.

Soit E un sous-ensemble de l'espace produit $X \otimes Y$. On appelle section de E par x, écrite E_x, l'ensemble des points y tels que :

$$(x, y) \in E.$$

De même, la section de E par y, notée E^y, est l'ensemble des points x tels que :

$$(x, y) \in E.$$

On sait que toute section d'un ensemble mesurable est un ensemble mesurable.

On obtient d'une façon analogue les sections d'une fonction f(x, y) définie sur l'espace produit $X \otimes Y$. On appelle section de f(x, y) par x, notée $f_x(y)$, la fonction définie sur Y par :

$$f_x(y) = f(x, y) .$$

La section de f(x, y) par y, notée $f^y(x)$, est la fonction définie sur X par:

$$f^y(x) = f(x, y) .$$

On sait que toute section d'une fonction mesurable est une fonction mesurable.

Si μ et ν sont deux mesures σ- finies respectivement sur $(X, \mathcal{X})$ et $(Y, \mathcal{Y})$, on obtient alors une mesure produite $\mu \otimes \nu$ sur l'espace produit $(X \otimes Y, \mathcal{X} \otimes \mathcal{Y})$. Pour tout ensemble mesurable $E \in \mathcal{X} \otimes \mathcal{Y}$ la mesure produite est définie par :

$$(\mu \otimes \nu)(E) = \int_X \nu(E_x)\, d\mu(x) = \int_Y \mu(E^y)\, d\nu(y)$$

A partir de ces définitions on a les lemmes suivants :

Lemme 1 :

Soient $(X, \mathcal{X})$ et $(Y, \mathcal{Y})$ deux espaces mesurables. Si f(x) est une fonction non-négative et mesurable $(\mathcal{X})$ et g(y) une fonction non-négative et mesurable $(\mathcal{Y})$, la fonction h(x, y) définie sur l'espace produit $X \otimes Y$ par :

$$h(x, y) = f(x). g(y)$$

est une fonction mesurable $(\mathcal{X} \otimes \mathcal{Y})$.

Lemme 2 :

Soient μ_1, ν_1 deux mesures définies sur $(X_1, \mathcal{X}_1)$ et μ_2, ν_2 deux mesures définies sur $(X_2, \mathcal{X}_2)$ telles que :

$$\nu_i << \mu_i \qquad i = 1, 2.$$

Si M, N sont des mesures produites :

$$M = \mu_1 \otimes \mu_2 \quad , \qquad N = \nu_1 \otimes \nu_2$$

définies sur $(X_1 \otimes X_2, \mathcal{X}_1 \otimes \mathcal{X}_2)$, on a : $N << M$.

Lemme 3 :

Si dans le lemme 2 on a : $d\nu_1 = f(x_1)\, d\mu_1$,

$d\nu_2 = g(x_2)\, d\mu_2$,

et $dN = h(x_1, x_2)\, dM$,

Alors, $h(x_1, x_2) = f(x_1). g(x_2)$

sauf sur un ensemble de M-mesure nulle.

DEFINITION DE LA LIGNE DE TRANSMISSION :

Dans le cas général que nous étudions une ligne de transmission est constituée par :

(i) Un espace mesurable $(X, \mathcal{X})$, l'espace des "lettres" à l'entrée

(ii) Un espace mesurable $(Y, \mathcal{Y})$, l'espace des "lettres" à la sortie

(iii) Une mesure de probabilité μ définie sur $(X, \mathcal{X})$, la probabilité selon laquelle sont choisies les lettres à l'entrée

(iv) Une famille de mesures de probabilité ν_x définies sur $(Y, \mathcal{Y})$ pour tout point $x \in X$. Cet ensemble de probabilités constitue le "bruit".

Nous supposerons de plus que pour tout ensemble $G \in \mathcal{Y}$, $\nu_x(G)$ considérée comme fonction de x est une fonction mesurable $(\mathcal{X})$. Nous avons alors le lemme et le théorème suivants. (Cf. Robbins (1948)).

Lemme 4 :

Pour tout ensemble $G \in \mathcal{Y}$, la fonction d'ensemble ν définie par :

$$\nu(G) = \int_X \nu_x(G)\, d\mu(x)$$

est une mesure de probabilité sur $(Y, \mathcal{Y})$.

THEOREME 2 :

Pour toute fonction non-négative et mesurable $(\mathcal{Y})$ $g(y)$ définie sur Y, la fonction de x :

$$\Phi(x) = \int_Y g(y)\, d\nu_x(y)$$

est une fonction non-négative et mesurable $(\mathcal{X})$, et :

$$\int_Y g(y)\, d\nu(y) = \int_X \Phi(x)\, d\mu(x) = \int_X d\mu(x) \int_Y g(y)\, d\nu_x(y)$$

Ce théorème s'étend facilement au cas où $g(y)$ est une fonction mesurable $(\mathcal{Y})$ non-nécessairement non-négative. Dans le cas où le domaine d'intégration est un ensemble mesurable $G \in \mathcal{Y}$, on a :

$$\int_G g(y)\, d\nu(y) = \int_X d\mu(x) \int_G g(y)\, d\nu_x(y)\,.$$

Considérons maintenant l'espace produit $(X \otimes Y, \mathcal{X} \otimes \mathcal{Y})$. Ayant défini la mesure ν, on peut définir sur cet espace la mesure produite $\mu \otimes \nu$. Mais nous définirons une autre mesure de probabilité λ sur cet espace produit à partir des mesures μ et ν_x.

Lemme 5 :

Pour tout ensemble mesurable $E \in \mathcal{X} \otimes \mathcal{Y}$, la fonction :

$$\nu_x(E_x)\,,$$

considérée comme fonction de x, est une fonction mesurable $(\mathcal{X})$.

Soit $\mathcal{A}$ la classe de tout ensemble mesurable E pour lequel le lemme est vrai. Soient $E^{(1)}$ et $E^{(2)}$ deux ensembles mesurables disjoints appartenant à $\mathcal{A}$.

Si $\quad E = E^{(1)} \cup E^{(2)}\,, \qquad$ on a : $\quad E_x = E_x^{(1)} \cup E_x^{(2)}$

et les ensembles $E_x^{(1)}$ et $E_x^{(2)}$ sont disjoints. On a donc :

$$\nu_x(E_x) = \nu_x(E_x^{(1)}) + \nu_x(E_x^{(2)})$$

$\nu_x(E_x)$ étant la somme de deux fonctions mesurables est, elle aussi, une fonction mesurable. Ainsi la réunion de deux ensembles disjoints appartenant à $\mathcal{A}$ appartient, elle aussi, à $\mathcal{A}$. Il est facile de voir que cela reste vrai pour la réunion d'un nombre dénombrable d'ensembles deux à deux disjoints.

Nous démontrerons que $\mathcal{A}$ est une classe monotone. C'est-à-dire que si nous avons une suite $\{E^{(n)}\}$ d'ensembles :

$$E^{(1)} \subset E^{(2)} \subset E^{(3)} \subset \ldots$$

appartenant tous à $\mathcal{A}$, la limite de cette suite appartient à $\mathcal{A}$. Soit :

$$E = \lim_{n\to\infty} E^{(n)} = \bigcup_n E^{(n)}$$

Ainsi E est un ensemble mesurable et on a :

$$E_x^{(1)} \subset E_x^{(2)} \subset E_x^{(3)} \ldots$$

et $E_x = \lim_{n\to\infty} E_x^{(n)} = \bigcup_n E_x^{(n)}$. Considérons la suite $\{\nu_x(E_x^{(n)})\}$. On a :

$$\nu_x(E_x^{(1)}) \leqslant \nu_x(E_x^{(2)}) \leqslant \ldots$$

$$\lim_{n\to\infty} \nu_x(E_x^{(n)}) = \nu_x(\lim_{n\to\infty} E_x^{(n)}) = \nu_x(E_x)$$

$\nu_x(E_x)$ étant la limite d'une suite non-décroissante de fonctions mesurables est une fonction mesurable, c'est-à-dire que :

$$E \in \mathcal{A}\ .$$

Par conséquent $\mathcal{A}$ est une classe monotone.

La classe $\mathcal{A}$ contient tous les rectangles mesurables, car pour tout ensemble $F \otimes G$, où $F \in \mathcal{X}$, $G \in \mathcal{Y}$, on a :

$$\nu_x\{(F \otimes G)_x\} = \nu_x(G)\ \chi_F(x)\ ;$$

$\nu_x(G)$ est mesurable par définition, $\chi_F(x)$ également puisqu'elle est la fonction caractéristique d'un ensemble mesurable et, par conséquent, $\nu_x(F \otimes G)_x$ est aussi une fonction mesurable.

Finalement, d'après le théorème bien connu (Halmos (1954), théorème 6B)

$$\mathcal{A} \supset \mathcal{X} \otimes \mathcal{Y}$$

ce qui complète la démonstration.

Lemme 6 :

La fonction d'ensemble λ définie pour tout ensemble mesurable E de l'espace produit par :

$$\lambda(E) = \int_X \nu_x(E_x)\, d\mu(x),$$

est une mesure de probabilité sur $(X \otimes Y, \mathcal{X} \otimes \mathcal{Y})$.

L'intégrale existe pour tout ensemble $E \in \mathcal{X} \otimes \mathcal{Y}$ car $\nu_x(E_x)$ est une fonction non-négative, mesurable et bornée. L'additivité de λ est une conséquence directe de l'additivité de la fonction ν_x. Finalement,

$$\lambda(X \otimes Y) = \int_X \nu_x(X \otimes Y)_x\, d\mu(x) = \int_X \nu_x(Y)\, d\mu(x) = 1.$$

Si l'ensemble E est un rectangle mesurable, soit $E = F \otimes G$, $F \in \mathcal{X}$, $G \in \mathcal{Y}$, on a :

$$\lambda(E) = \lambda(F \otimes G) = \int_F \nu_x(G)\, d\mu(x).$$

Lemme 7 :

Pour toute fonction $h(x, y)$ non-négative et mesurable $(\mathcal{X} \otimes \mathcal{Y})$ la fonction :

$$f(x) = \int_Y h(x, y)\, d\nu_x(y)$$

est une fonction non-négative et mesurable $(\mathcal{X})$.

La fonction $f(x)$ est évidemment non-négative. Examinons la question de mesurabilité. Si $h(x, y)$ est la fonction caractéristique $\chi_F(x, y)$ d'un ensemble mesurable $E \in \mathcal{X} \otimes \mathcal{Y}$, on a :

$$f(x) = \int_Y \chi_F(x, y)\, d\nu_x(y) = \int_Y \chi_{E_x}(y)\, d\nu_x(y) = \nu_x(E_x)$$

La fonction $f(x)$ est donc mesurable dans ce cas. De même, il est évident que $f(x)$ est mesurable dans le cas où $h(x, y)$ est une fonction non-négative simple.

Si $h(x, y)$ est une fonction mesurable non-négative quelconque, il existe une suite $\{h_n(x, y)\}$ de fonctions non-négatives simples qui est non-décroissante et qui converge partout à la fonction $h(x, y)$. Posons :

$$f_n(x) = \int_Y h_n(x, y)\, d\nu_x(y)$$

Ainsi pour toute fonction $h(x, y)$, la fonction correspondante $f_n(x)$ est mesurable. La suite $\{f_n(x)\}$ est une suite non-décroissante de fonctions non-négatives mesurables et nous avons :

$$f(x) = \lim_{n\to\infty} f_n(x)$$
$$= \lim_{n\to\infty} \int_Y h_n(x, y)\, d\nu_x(y)$$
$$= \int_Y h(x, y)\, d\nu_x(y)$$

Ainsi la fonction f(x) est aussi une fonction mesurable et le lemme est démontré.

THEOREME 3 :

La mesure λ est telle que pour toute fonction h(x, y) non-négative et mesurable $(\mathcal{X} \otimes \mathcal{Y})$

$$\int_{X\otimes Y} h(x, y)\, d\lambda(x, y) = \int_X d\mu(x) \int_Y h(x, y)\, d\nu_x(y)$$

Pour tout ensemble mesurable $E \in \mathcal{X} \otimes \mathcal{Y}$ nous avons :

$$\int_X d\mu(x) \int_Y \chi_F(x, y)\, d\nu_x(y) = \int_X d\mu(x) \int_Y \chi_{F_x}(y)\, d\nu_x(y) =$$

$$= \int_X \nu_x(E_x)\, d\mu(x) = \lambda(E) = \int_{X\otimes Y} \chi_E(x, y)\, d\lambda(x, y)$$

Le théorème est donc valable pour les fonctions caractéristiques d'ensembles mesurables. De même il est vrai pour les fonctions non-négatives simples. Et finalement, en considérant pour toute fonction non-négative mesurable une suite non-décroissante de fonctions non-négatives simples qui converge partout à cette fonction, on voit que le théorème est toujours valable.

Si au lieu de l'espace tout entier $X \otimes Y$ on prend comme domaine d'intégration un ensemble mesurable $E \in \mathcal{X} \otimes \mathcal{Y}$, on a :

$$\int_E h(x, y)\, d\lambda(x, y) = \int_X d\mu(x) \int_{E_x} h(x, y)\, d\nu_x(y).$$

Les théorèmes et les lemmes que nous avons énoncés ci-dessus pour les fonctions mesurables non-négatives, s'étendent facilement aux fonctions mesurables.

Considérons maintenant un lemme qui généralise un lemme de Feinstein (1954, lemme 2) et qui nous servira pour la démonstration du théorème foncamental.

Lemme 8 :

Soient α, δ deux nombres positifs arbitrairement petits. Soit $E \in \mathcal{X} \otimes \mathcal{Y}$ un ensemble mesurable de l'espace produit $X \otimes Y$. Si :

$$\lambda(E) > 1 - \delta$$

et si F est l'ensemble des points $x \in X$ pour lesquels :

$$\nu_x(E_x) > 1 - \alpha \quad ,$$

on a :

$$\mu(F) \geqslant 1 - \frac{\delta}{\alpha} .$$

Soit $\overline{F}$ l'ensemble complémentaire de F par rapport à X et soit $\overline{E}_x$ l'ensemble complémentaire de E_x par rapport à Y. On a alors :

$$\nu_x(E_x) + \nu_x(\overline{E}_x) = 1 .$$

Pour tout $x \in \overline{F}$ on a :

$$\nu_x(E_x) \leqslant 1 - \alpha$$

et donc :

$$\nu_x(\overline{E}_x) > \alpha \quad . \text{ D'où } \quad \int_{\overline{F}} \nu_x(\overline{E}_x)\, d\mu(x) > \alpha\, \mu(\overline{F}) .$$

Mais :

$$\int_F \nu_x(\overline{E}_x)\, d\mu(x) \leqslant \int_X \nu_x(\overline{E}_x)\, d\mu(x)$$

$$= \lambda(\overline{E}) \qquad (\text{car } \overline{E}_x = (\overline{E})_x$$

$$\leqslant \delta .$$

Ce qui donne :

$$\alpha\, \mu(\overline{F}) < \delta \;, \qquad \text{c'est-à-dire : } \quad \mu(F) \geqslant 1 - \frac{\delta}{\alpha} .$$

C.Q.F.D.

Nous pouvons maintenant définir la capacité de la ligne de transmission dans le cas général. Pour que cette définition soit utile il faut que la mesure λ soit absolument continue par rapport à la mesure produite $\mu \otimes \nu$; et pour cela des conditions supplémentaires sont nécessaires. Ces conditions supplémentaires, on peut les choisir de diverses manières et, afin de rendre les choses plus simples, nous supposerons que les mesures ν_x constituent une famille homogène, c'est-à-dire que :

$$\nu_{x_1} \ll \nu_{x_2} \;,\quad \nu_{x_2} \ll \nu_{x_1}$$

pour tout couple x_1, x_2 appartenant à X. (Cf. Halmos et Savage, (1949))

THEOREME 4 :

Si les mesures ν_x constituent une famille homogène, la mesure λ est absolument continue par rapport à la mesure produite $\mu \otimes \nu$.

Pour tout ensemble $G \in \mathcal{Y}$, on a :

$$\nu(G) = \int_X \nu_x(G)\, d\mu(x) .$$

Si $\nu(G)$ est égale à zéro, la fonction $\nu_x(G)$ de x étant une fonction non-négative est, elle aussi, égale à zéro pour tout point $x \in X$ à l'exception d'un ensemble de μ-mesure nulle. Comme les mesures ν_x constituent une famille homogène il s'en suit que $\nu_x(G) = 0$ pour tout x.

Soit maintenant E un ensemble mesurable de l'espace produit $(X \otimes Y, \mathcal{X} \otimes \mathcal{Y})$ tel que l'on ait :

$$(\mu \otimes \nu)(E) = \int_X \nu(E_x)\, d\mu(X) = 0.$$

On a alors,

$$\nu(E_x) = 0$$

pour tout $x \in X$ sauf pour un ensemble de μ-mesure nulle. D'après ce que nous venons de dire plus haut il suit que :

$$\nu_x(E_x) = 0$$

sauf pour un ensemble de μ-mesure nulle, et donc que,

$$\lambda(E) = \int_X \nu_x(E_x)\, d\mu(x) = 0,$$

ce qui démontre le théorème.

Soit f(x, y) la dérivée de Radon-Nikodym de λ par rapport à $\mu \otimes \nu$. f(x, y) est une fonction non-négative, mesurable et bornée. On sait que la dérivée de Radon-Nikodym n'est définie qu'à un ensemble de mesure nulle près. Nous supposerons que parmi toutes les déterminations possibles de la dérivée, une détermination a été choisie et que f(x, y) la désigne.

Pour toute mesure de probabilité μ définie sur l'espace $(X, \mathcal{X})$, on définit alors le débit de transmission $R(\mu)$ par :

$$R(\mu) = \int_{X \otimes Y} \operatorname{Log} f(x, y)\, d\lambda(x, y)$$

Cette définition n'est valable que pour le cas où cette intégrale existe.

Soit maintenant $\mathfrak{M}$ la famille des mesures de probabilité μ pour lesquelles cette intégrale existe. Les mesures de cette famille sont des mesures possibles à l'entrée et donc cette famille fait partie de la définition-même de la ligne. Relativement à cette famille $\mathfrak{M}$, on définit alors la capacité C par :

$$C = \operatorname*{Sup}_{\mu \in \mathfrak{M}} R(\mu)$$

Avant d'établir certaines propriétés de R analogues à celles étudiées par Shannon, nous allons donner quelques résultats qui seront utilisés ultérieurement.

Considérons la section de f(x, y) par un point $y \in Y$ quelconque. La section $f^y(x)$ est une fonction mesurable ($\mathfrak{X}$), non-négative et bornée. Donc l'intégrale :

$$\int_F f^y(x)\, d\mu(x)$$

existe pour tout ensemble mesurable $F \in \mathfrak{X}$.

Lemme 9 :

La fonction d'ensemble μ^y définie sur $(X, \mathfrak{X})$ pour tout point $y \in Y$ par :

$$\mu^y(F) = \int_F f^y(x)\, d\mu(x) \quad , \quad F \in \mathfrak{X}$$

est une fonction mesurable ($\mathfrak{Y}$) pour tout ensemble $F \in \mathfrak{X}$, et une mesure de probabilité sur $(X, \mathfrak{X})$ pour presque tout y.

Que $\mu^y(F)$ soit une fonction mesurable ($\mathfrak{X}$) pour tout ensemble $F \in \mathfrak{X}$, cela est une conséquence du théorème de Fubini. Pour démontrer la seconde partie du lemme nous avons, pour tout ensemble $G \in \mathfrak{Y}$

$$\int_{X \otimes G} f(x, y)\, d(\mu \otimes \nu)(x, y) = \int_G d\nu(y) \int_X f^y(x)\, d\mu(x)$$
$$= \int_G \mu^y(X)\, d\nu(y)$$

Mais :

$$\int_{X \otimes G} f(x, y)\, d(\mu \otimes \nu)(x, y) = \lambda(X \otimes G) = \int_X \nu_x(G)\, d\mu(x) = \nu(G)$$

Ainsi, pour tout ensemble $G \in \mathfrak{Y}$, on a :

$$\int_G \mu^y(X)\, d\nu(y) = \nu(G)$$

Par conséquent :

$$\mu^y(X) = 1 ,$$

pourtout point $y \in Y$, à l'exception d'un ensemble de ν-mesure nulle ; ce qui démontre le lemme.

Si l'on considère la section $f_x(y)$, on obtient le lemme suivant qui se démontre de la même façon.

Lemme 10 :

La fonction d'ensemble η_x définie sur $(Y, \mathcal{Y})$ pour tout point $x \in X$ par :

$$\eta_x(G) = \int_G f_x(y)\, d\nu(y), \qquad G \in \mathcal{Y}$$

est une fonction mesurable $(\mathcal{X})$ pour tout ensemble $G \in \mathcal{Y}$, et une mesure de probabilité sur $(Y, \mathcal{Y})$ pour presque tout x.

PROPRIETES DE LA CAPACITE C :

Nous allons démontrer deux propriétés du débit de transmission $R(\mu)$ et on pourra en déduite les propriétés de C.

1/ - $R(\mu) \geqslant 0$:

Cette propriété découle du théorème suivant sur les fonctionnelles convexes (Hardy, Littlewood, Polya (1934), p. 151).

THEOREME 5 :

Soit μ une mesure de probabilité définie sur un espace mesurable $(X, \mathcal{X})$. Si $f(x)$ est une fonction mesurable $(\mathcal{X})$ telle que :

(i) $\alpha \leqslant f(x) \leqslant \beta$, α et β peuvent être ou non bornés.

(ii) $f(x)$ est presque partout différent de α et de β, et si $\Phi(t)$ est une fonction définie sur l'intervalle $\alpha < t < \beta$, telle que $\Phi''(t)$ est positive et finie pour $\alpha < t < \beta$, alors, on a :

$$\Phi\left\{\int_X f(x)\, d\mu(x)\right\} \leqslant \int_X \Phi(f)\, d\mu(x) ,$$

à condition que l'intégrale :

$$\int_X f(x)\, d\mu(x)$$

existe. On a l'égalité si, et seulement si, f(x) est partout égale à une constante.

Si l'on prend un ensemble mesurable $E \in \mathscr{X}$ comme domaine d'intégration au lieu de l'espace X tout entier, on a :

$$\Phi \left\{ \frac{\int_E f(x)\, d\mu\, (x)}{\mu(E)} \right\} \leq \frac{\int_E \Phi\, (f)\, d\mu\, (x)}{\mu\, (E)}$$

Nous avons :

$$R(\mu) = \int_{X \otimes Y} \text{Log}\, f(x,\, y)\, d\lambda\, (x,\, y)$$

$$= \int_{X \otimes Y} f(x,\, y)\, \text{Log}\, f(x,\, y)\, d\, (\mu \otimes \nu)(x,\, y)\, ,$$

et $\int_{X \otimes Y} f(x,\, y)\, d(\mu \otimes \nu)(x,\, y) = \lambda\, (X \otimes Y) = 1\, .$

Si dans le théorème ci-dessus, on prend :

$$\Phi\, (t) = t\, \text{Log}\, t$$

On obtient :

$$R(\mu) = \int \Phi\, (f)\, d(\mu \otimes \nu)$$

$$\geq \Phi\, (1) = 0\, .$$

De plus, $R(\mu) = 0$ si, et seulement si, $f(x, y) = 1$ partout, c'est-à-dire si les deux mesures λ et $\mu \otimes \nu$ sont identiques.

2/ - La fonction R est additive pour les espaces produits :

Considérons l'espace à 2n dimensions dont tous point ξ est une suite de n couples :

$$(x_1,\, y_1),\, (x_2,\, y_2)\, ,\, \ldots\, ,\, (x_n,\, y_n)$$

où $x_i \in X$, $y_i \in Y$. On peut le considérer comme l'espace produit à n dimensions de l'espace $X \otimes Y$ avec lui-même, c'est-à-dire que l'on peut le représenter comme :

$$\prod_{i=1}^{n} (X_i \otimes Y_i) = (X_1 \otimes Y_1) \otimes (X_2 \otimes Y_2) \otimes \ldots \otimes (X_n \otimes Y_n)$$

où $X_i = X\, ,\; Y_i = Y\, ,\; i = 1,\, 2,\, \ldots\, ,\, n\, .$

Le corps borélien correspondant s'écrit :

$$\prod_{i=1}^{n} (\mathscr{X}_i \otimes \mathscr{Y}_i) = (\mathscr{X}_1 \otimes \mathscr{Y}_1) \otimes (\mathscr{X}_2 \otimes \mathscr{Y}_2) \otimes \ldots \otimes (\mathscr{X}_n \otimes \mathscr{Y}_n)$$

où $\mathcal{X}_i = \mathcal{X}, \quad \mathcal{Y}_i = \mathcal{Y}, \quad i = 1, 2, \dots, n.$

A partir de cette représentation on peut définir une mesure produite :

$$\Lambda = \lambda_1 \otimes \lambda_2 \otimes \dots \otimes \lambda_n \ ; \ i = 1, 2, \dots, n.$$

Λ est aussi une mesure de probabilité. De même on peut définir une autre mesure de probabilité :

$$\Omega = (\mu_1 \otimes \nu_1) \otimes \dots \otimes (\mu_n \otimes \nu_n),$$

avec : $\left.\begin{array}{l} \mu_i = \mu \\ \nu_i = \nu \end{array}\right\} \quad i = 1, 2, \dots, n.$

D'après le lemme 2, on a : $\Lambda \ll \Omega$,

et si l'on désigne par $\Psi(\xi)$ la dérivée de Radon-Nikodym de Λ par rapport à Ω, on a(cf. lemme 3) :

$$\Psi(\xi) = \prod_{i=1}^{n} f(x_i, y_i)$$

où $\xi = ((x_1, y_1), (x_2, y_2), \dots, (x_n, y_n))$

Par conséquent :

$$\int \text{Log}\, \Psi(\xi)\, d\Lambda = \int \left[\sum_i \text{Log}\, f(x_i, y_i)\right] d\Lambda$$
$$= \sum_i \int_{X_i \otimes Y_i} \text{Log}\, f(x_i, y_i)\, d\lambda(x_i, y_i) = nR.$$

ce qui démontre la seconde propriété.

La propriété d'additivité nous donne, d'après la loi des grands nombres, le théorème suivant.

THEOREME 6 :

Soient ε, δ deux nombres positifs arbitrairement petits. On peut alors trouver un nombre entier $n_0(\varepsilon, \delta)$ tel que pour tout nombre entier $n \geqslant n_0$

$$\Pr\left\{ \left| \frac{1}{n} \text{Log}\, \Psi(\xi) - R \right| < \varepsilon \right\} \geqslant 1 - \delta .$$

C'est-à-dire que pour n suffisamment grand, l'espace produit à 2n dimensions $(\prod_i (X_i \otimes Y_i), \prod_i (\mathcal{X}_i \otimes \mathcal{Y}_i))$ se décompose en deux ensembles mesurables $W^{(\delta)}$, et $\overline{W}^{(\delta)}$ (l'ensemble complémentaire), tels que :

$$\Lambda(W^{(\delta)}) \geqslant 1 - \delta$$

et que, pour tout $\xi \in W^{(\delta)}$:

$$\left| \frac{1}{n} \operatorname{Log} \Psi(\xi) - R \right| < \varepsilon$$

c'est-à-dire que :

$$e^{n(R-\epsilon)} < \Psi(\xi) < e^{n(R+\epsilon)} .$$

LE THEOREME FONDAMENTAL :

Considérons de plus près l'espace produit à 2n dimensions $(\prod_i (X_i \otimes Y_i), \prod_i (\mathfrak{X}_i \otimes \mathfrak{Y}_i))$. Notre notation signifie que nous considérons tout point ξ de cet espace comme une suite de couples,

$$\xi = ((x_1, y_1), (x_2, y_2), \ldots , (x_n, y_n)).$$

Les mesures Λ et Ω sont définies par rapport à cette représentation. Mais tout point de cet espace à 2n dimensions peut être aussi considéré comme un couple de suites (u, v) où :

$$u = (x_1, x_2, \ldots , x_n)$$

$$v = (y_1, y_2, \ldots , y_n)$$

Dans ce cas, si $(U, \mathfrak{U})$ et $(V, \mathfrak{V})$ représentent respectivement les espaces produits à n dimensions de $(X, \mathfrak{X})$ et de $(Y, \mathfrak{Y})$ avec eux-mêmes, c'est-à-dire si :

$$(U, \mathfrak{U}) = (X_1 \otimes \ldots \otimes X_n, \mathfrak{X}_1 \otimes \ldots \otimes \mathfrak{X}_n)$$

et $$(V, \mathfrak{V}) = (Y_1 \otimes \ldots \otimes Y_n, \mathfrak{Y}_1 \otimes \ldots \otimes \mathfrak{Y}_n)$$

ou $X_i = X,\ Y_i = Y,\ \mathfrak{X}_i = \mathfrak{X},\ \mathfrak{Y}_i = \mathfrak{Y}, \quad i = 1, 2, \ldots , n ,$

l'espace produit à 2n dimensions peut être représenté comme l'espace produit $U \otimes V$ de points (u, v) avec le corps borélien $\mathfrak{U} \otimes \mathfrak{V}$.

A partir de cette nouvelle représentation on peut définir les mesures produites qui sont des mesures de probabilité :

$$M = \mu_1 \otimes \mu_2 \otimes \ldots \otimes \mu_n , \qquad \mu_i = \mu$$

$$N = \nu_1 \otimes \nu_2 \otimes \ldots \otimes \nu_n , \qquad \nu_i = \nu$$

respectivement sur $(U, \mathcal{U})$ et $(V, \mathcal{V})$. De même, pour tout point :

$$u = (x_1, x_2, \ldots, x_n)$$

de l'espace U, on peut définir une mesure :

$$N_u = \nu_{x_1} \otimes \nu_{x_2} \otimes \ldots \otimes \nu_{x_n} \qquad \text{sur } (V, \mathcal{V}).$$

Les mesures N_u ont des propriétés analogues à celles des mesures ν_x, à savoir, pour tout point $u \in U$, N_u est une mesure de probabilité sur $(V, \mathcal{V})$ et, pour tout ensemble mesurable $G \in \mathcal{V}$, $N_u(G)$ est une fonction mesurable $(\mathcal{U})$ définie sur U. La première propriété est évidente. Pour démontrer la seconde il suffit de considérer la famille $\mathcal{F}$ d'ensembles $G \in \mathcal{V}$ pour lesquels $N_u(G)$ a cette propriété. On voit facilement que $\mathcal{F}$ contient la réunion de toute suite dénombrable d'ensembles disjoints ainsi que la limite de toute suite monotone d'ensembles appartenant à $\mathcal{F}$. Comme $\mathcal{F}$ contient évidemment tous les "rectangles" mesurables de la forme :

$$G = G_1 \otimes G_2 \otimes \ldots \otimes G_n, \; G_i \in \mathcal{V},$$

elle contient forcément le corps borélien $\mathcal{V}$. Par conséquent, pour tout ensemble $G \in \mathcal{V}$, la fonction $N_u(G)$ de u est mesurable $(\mathcal{U})$.

A partir de la mesure M définie sur $(U, \mathcal{U})$ et de la famille de mesures N_u définies sur $(V, \mathcal{V})$, on peut définir une autre mesure de probabilité $\overline{N}$ sur $(V, \mathcal{V})$ par :

$$\overline{N}(G) = \int_U N_u(G)\, dM(u), \quad G \in \mathcal{V}.$$

(cf. lemme 4). La mesure $\overline{N}$ ainsi définie s'identifie avec la mesure N définie plus haut. Plus précisément, pour tout ensemble $G \in \mathcal{V}$, on a :

$$\overline{N}(G) = N(G).$$

La relation est vraie pour tout "rectangle" mesurable.

$$G = G_1 \otimes G_2 \otimes \ldots G_n, \quad G_i \in \mathcal{V},$$

car :

$$\begin{aligned} \overline{N}(G) &= \int_U N_u(G)\, dM(u) \\ &= \int_X \ldots \int_X \nu_{x_1}(G_1)\, \nu_{x_2}(G_2) \ldots \nu_{x_n}(G_n)\, d(\mu_1 \otimes \ldots \otimes \mu_n)(x_1, \ldots, x_n) \\ &= \prod_{i=1}^{n} \int_X \nu_{x_i}(G_i)\, d\mu(x_i) = \prod_{i=1}^{n} \nu(G_i) = N(G). \end{aligned}$$

Elle est évidemment vraie pour toute réunion d'un nombre fini de "rectangles" mesurables disjoints. Par conséquent, elle est vraie pour tout ensemble mesurable $G \in \mathcal{V}$.

Nous voyons donc que ces mesures M, N, et N_u sont liées entre elles par les relations du même genre que celles qui existaient entre les mesures μ, ν et ν_x. Ainsi tout théorème démontré pour ces dernières resterait valable pour les premières. Par exemple, pour toute fonction g(v) non-négative et mesurable ($\mathcal{V}$), on a :

$$\int_G g(v)\, dN(v) = \int_U dM(u) \int_G g(v)\, dN_u(v), \quad G \in \mathcal{V} .$$

(cf. théorème 2). De même, pour tout ensemble mesurable $E \in \mathcal{U} \otimes \mathcal{V}$ de l'espace produit $U \otimes V$, la fonction $N_u(E_u)$ de u est mesurable ($\mathcal{U}$)(cf. lemme 5). Ceci nous permet de définir une mesure de probabilité L sur $(U \otimes V, \mathcal{U} \otimes \mathcal{V})$. Comme la mesure λ, la mesure L se définit par :

$$L(E) = \int_U N_u(E_u)\, dM(u), \qquad E \in \mathcal{U} \otimes \mathcal{V}.$$

Pour toute fonction h(u, v) non-négative et mesurable ($\mathcal{U} \otimes \mathcal{V}$), on a :

$$\int_E h(u,v)\, dL(u,v) = \int_U dM(u) \cdot \int_{E_u} h(u,v)\, dN_u(v), \quad E \in \mathcal{U} \otimes \mathcal{V}$$

(cf. théorème 3). Et finalement, la mesure L est absolument continue par rapport à $M \otimes N$ (cf. théorème 4).

Les mesures L et $M \otimes N$ sont respectivement identiques, dans un certain sens, aux mesures Λ et Ω. La correspondance qui à chaque point :

$$(x_1, x_2, \ldots , x_n ; y_1, y_2, \ldots , y_n)$$

de l'espace $U \otimes V$ associe le point :

$$((x_1, y_1), (x_2, y_2), \ldots , (x_n, y_n))$$

de l'espace $\prod_i (X_i \otimes Y_i)$, définit une transformation bi-univoque entre les espaces mesurables $(U \otimes V, \mathcal{U} \otimes \mathcal{V})$ et $(\prod_i (X_i \otimes Y_i), \prod_i (\mathcal{X}_i \otimes \mathcal{Y}_i))$. Cette transformation, ainsi que son inverse, est une transformation mesurable et elle conserve la mesure en ce sens que l'image E^* de tout ensemble E appartenant à $\mathcal{U} \otimes \mathcal{V}$ appartient à $\prod_i (\mathcal{X}_i \otimes \mathcal{Y}_i)$ et que :

$$L(E) = \Lambda(E^*) \quad , \qquad (M \otimes N)(E) = \Omega(E^*)$$

Si l'on considère maintenant sur l'espace $(U \otimes V, \mathcal{U} \otimes \mathcal{V})$ la fonction :

$$\Phi(u, v) = \Psi(\xi)$$

où $u = (x_1, x_2, \ldots, x_n)$, $v = (y_1, y_2, \ldots, y_n)$

et $\xi = ((x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n))$

on voit facilement, d'après la discussion sur les deux représentations différentes de l'espace produit à 2n dimensions, que :

$$L(E) = \int_E \Phi(u, v)\, d(M \otimes N)(u, v)$$

pour tout ensemble mesurable $E \in \mathcal{U} \otimes \mathcal{V}$. La fonction $\Phi(u, v)$ peut donc être considérée comme une des déterminations de la dérivée de Radon-Nikodym de la mesure L par rapport à $M \otimes N$. On a aussi :

$$\int_{U \otimes V} \operatorname{Log} \Phi(u, v)\, dL(u, v) = nR$$

On peut également réinterpréter le résultat découlant de la loi des grands nombres pour ce cas. En effet, on peut dire qu'étant donnés deux nombres positifs ϵ et δ arbitrairement petits, l'espace $U \otimes V$ se décompose, pour n suffisamment grand, en deux ensembles que nous noterons toujours par $W^{(\delta)}$ et $\bar{W}^{(\delta)}$, tels que :

$$L(W^{(\delta)}) \geqslant 1 - \delta \quad ,$$

et que : $$e^{n(R-\epsilon)} < \Phi(u, v) < e^{n(R+\epsilon)}$$

pour tout point $(u, v) \in W^{(\delta)}$. On peut maintenant démontrer le théorème suivant :

THEOREME 7 :

Pour n suffisamment grand :

$$(1 - \delta)\, e^{-n(R+\epsilon)} < (M \otimes N)(W^{(\delta)}) < e^{-n(R-\epsilon)} .$$

Pour tout point $(u, v) \in W^{(\delta)}$, on a :

$$e^{n(R-\epsilon)} < \Phi(u, v) < e^{n(R+\epsilon)}$$

D'où : $$e^{n(R-\epsilon)} (M \otimes N)(W^{(\delta)}) < \int_{W^{(\delta)}} \Phi(u, v)\, d(M \otimes N)(u, v) < e^{n(R+\epsilon)} (M \otimes N)(W^{(\delta)}) ,$$

c'est-à-dire :

$$(M \otimes N)(W^{(\delta)})\, e^{n(R-\epsilon)} < L(W^{(\delta)}) < (M \otimes N)(W^{(\delta)})\, e^{n(R+\epsilon)}$$

Si l'on considère maintenant les inégalités :

$$1 - \delta \leqslant L(W^{(\delta)}) \leqslant 1$$

on obtient le résultat voulu.

Considérons maintenant l'intégrale :

$$\int_G \Phi(u, v)\, dN(v), G \in \mathcal{V} .$$

D'après le lemme 10, cette intégrale définit, pour tout point $u \in U$, à l'exception d'un ensemble de M-mesure nulle, une mesure de probabilité sur $(V, \mathcal{V})$.

THEOREME 8 :

Si l'on désigne par $W_u^{(\delta)}$ la section par le point u de l'ensemble $W^{(\delta)}$ alors, pour n suffisamment grand, on a :

$$N(W_u^{(\delta)}) < e^{-n(R-\epsilon)}$$

pour tout $u \in U$, à l'exception d'un ensemble de M-mesure nulle.

En effet, pour tout point $u \in U$ pour lequel $W_u^{(\delta)}$ n'est pas vide, on a :

$$e^{n(R-\epsilon)} < \Phi(u, v) < e^{n(R+\epsilon)}$$

D'où :

$$N(W_u^{(\delta)})\, e^{n(R-\epsilon)} < \int_{W_u} \Phi(u, v)\, dN(v) < N(W_u^{(\delta)})\, e^{n(R+\epsilon)}$$

Mais pour presque tout point $u \in U$, on a :

$$\int_{W_u^{(\delta)}} \Phi(u, v)\, dN(v) \leqslant 1.$$

Par conséquent :

$$N(W_u^{(\delta)}) < e^{-n(R-\epsilon)}$$

Par contre, si le point $u \in U$ est tel que l'ensemble $W_u^{(\delta)}$ est vide, ce résultat est évidemment vrai. Le théorème est ainsi démontré.

Nous pouvons maintenant entreprendre la démonstration d'un théorème analogue au théorème fondamental de la théorie de l'information. Le raisonnement utilisé sera celui qu'emploie Feinstein (1954) ; (voir aussi Khintchine (1956)). Le théorème 8 qui nous servira à notre dé-

monstration n'étant valable que pour les points u à l'extérieur d'un ensemble de M-mesure nulle, nous supposerons, dans tout ce qui suit, que cet ensemble de mesure nulle n'est pas pris en considération. Ainsi toutes les fois que l'on parlera d'une propriété vraie pour tout point $u \in U$, il sera sous-entendu qu'il s'agit de tout point u à l'exception de cet ensemble.

Soit C la capacité de la ligne de transmission. Par définition il existe une mesure de probabilité $\mu \in \mathcal{M}$ définie sur $(X, \mathcal{X})$ telle que :

$$R(\mu) > C - \frac{\theta}{2},$$

où θ est un nombre positif arbitrairement petit. Ayant choisi μ on obtient les mesures ν et λ. Soit L, M, N, et N_u les mesures de probabilité correspondantes sur l'espace produit $(U \otimes V, \mathcal{U} \otimes \mathcal{V})$.

Ainsi, d'après le théorème résultant de la loi des grands nombres (théorème 6) on peut trouver, pour n suffisamment grand, un sous-ensemble $W \subseteq U \otimes V$ tel que :

(i) $L(W) > 1 - \frac{\theta^2}{2}$,

(ii) $e^{n(R-\frac{\theta}{2})} < \Phi(u, v) < e^{n(R+\frac{\theta}{2})}$

pour tout point $(u, v) \in W$.

Et, d'après le lemme de Feinstein (lemme 8), si F est l'ensemble des points u pour lesquels :

$$N_u(W_u) > 1 - \frac{\theta}{2},$$

on a :

$$M(F) \geqslant 1 - \theta .$$

Soient maintenant $\tilde{F}_1, \tilde{F}_2, \ldots, \tilde{F}_m$ les ensembles deux à deux disjoints, pour lesquels les conditions suivantes sont satisfaites.

1/ - Pour tout $\tilde{F}_j$ $(j = 1, 2, \ldots, m)$, il existe un ensemble B_j tel que :

$$N_u(B_j) \geqslant 1 - \theta$$

pour tout point $u \in \tilde{F}_j$, c'est-à-dire :

$$\frac{1}{M(\tilde{F}_j)} \int_{\tilde{F}_j} N_u(B_j)\, dM(u) \geq 1 - \theta$$

2/ - $N(B_j) < e^{-n(R-\frac{\theta}{2})}$

3/ - Les ensembles B_j sont deux à deux disjoints.

4/ - La famille $\{ \tilde{F}_1, \tilde{F}_2, \ldots, \tilde{F}_m \}$ est une famille maximale, c'est-à-dire que si l'on y ajoutait un autre ensemble, l'une au moins des trois premières conditions serait violée.

THEOREME 9 (Le théorème fondamental) :

Pour n suffisamment grand, on a:

$$m > e^{n(C-2\theta)}$$

Posons :

$$\tilde{F} = \tilde{F}_1 \cup \tilde{F}_2 \cup \ldots \cup \tilde{F}_m .$$

Et pour tout $u \in F - \tilde{F}$ (à condition que l'ensemble $F - \tilde{F}$ ne soit pas vide) considérons l'ensemble :

$$\mathcal{E}_u = W_u - W_u \cap (\bigcup_j B_j)$$

$$= W_u - W_u \cap B \qquad (B = \bigcup_j B_j)$$

On voit que $\mathcal{E}_u$ est disjoint de tous les B_j et que :

$$N(\mathcal{E}_u) \leq N(G_i) < e^{-n(R-\frac{\theta}{2})} \qquad \text{(Théorème 8)}$$

Comme la famille $\{ \tilde{F}_j \,; j = 1, 2, \ldots, m \}$ est une famille maximale, on devrait donc avoir (si l'on suppose que tout ensemble d'un seul point u est mesurable).

$$N_u(\mathcal{E}_u) < 1 - \theta$$

pour tout point $u \in F - \tilde{F}$. C'est-à-dire :

$$N_u(W_u) - N_u(W_u \cap B) < 1 - \theta$$

$$N_u(W_u \cap B) > N_u(W_u) - (1 - \theta) > (1 - \frac{\theta}{2}) - (1 - \theta) = \frac{\theta}{2} .$$

C'est-à-dire $N_u(B) > \frac{\theta}{2}$,

pour tout point $u \in F - \tilde{F}$. Par contre, pour $u \in \tilde{F}$, on a :

$$N_u(B) \geqslant 1 - \theta \ ,$$

tel que :

$$N(B) = \int_U N_u(B)\, dM(u) \geqslant \int_{F-\tilde{F}} N_u(B)\, dM(u) + \int_{\tilde{F}} N_u(B)\, dM(u)$$

$$> \frac{\theta}{2} M(F - \tilde{F}) + (1 - \theta) M(\tilde{F}) = \frac{\theta}{2} M(F) + (1 - \frac{\theta}{2})\, M(\tilde{F})$$

$$> \frac{\theta}{2} M(F) \quad (\text{si } \frac{\theta}{2} < 1)\ , \ > \frac{\theta}{2}(1 - \theta) \qquad (\text{car } M(F) \geqslant 1 - \theta)$$

D'autre part : $N(B) \sum_{j=1}^{m} N(B_j) < m e^{-n(R - \frac{\theta}{2})}$

et par conséquent :

$$m > \frac{\theta}{2} (1 - \theta)\, e^{n(R - \frac{\theta}{2})}$$

$$> \frac{\theta}{2} (1 - \theta)\, e^{n(C - \theta)}$$

que l'on peut finalement écrire :

$$m > e^{n(C - 2\theta)}$$

ce qui échève la démonstration.

Ainsi, pour n suffisamment grand, on peut trouver un nombre $m > e^{n(C-2\theta)}$ de sous-ensembles $\tilde{F}_j$ deux à deux disjoints tels que la probabilité conditionnelle pour que le message reçu v se trouve dans le sous-ensemble B_j lorsque le message transmis u appartient à $\tilde{F}_j$ est très proche de l'unité car :

$$\frac{1}{M(\tilde{F}_j)} \int_{\tilde{F}_j} N_u(B_j)\, dM(u) \geqslant 1 - \theta \ .$$

Les sous-ensembles B_j sont, eux aussi, deux à deux disjoints, et ainsi chaque fois qu'un message reçu v appartient à un sous-ensemble B_j on peut être sûr que le message transmis u appartenait au sous-ensemble $\tilde{F}_j$, l'erreur totale d'identification étant inférieure à θ.

CHAPITRE IV

L'INFORMATION EN STATISTIQUE MATHÉMATIQUE

L'INFORMATION DE FISHER -

C'est M. Fisher qui a introduit pour la première fois le concept d'information en statistique mathématique. Il définit l'information $I(\theta)$, associée à la densité de probabilité $f(x, \theta)$, par :

$$I(\theta) = \int_{-\infty}^{\infty} \frac{1}{f(x, \theta)} \left[\frac{\partial f(x, \theta)}{\partial \theta}\right]^2 dx$$

Fisher se plaçait dans le cadre d'un problème précis, celui de l'estimation des paramètres d'une densité de probabilité. Sa fonction d'information est ainsi intimement liée à sa théorie d'estimation ou plus précisément à deux notions, celle de la précision d'une estimation et celle d'un résumé exhaustif.

Dans la théorie fishérienne de l'estimation, la précision d'une estimation est mesurée par l'inverse de la variance de l'estimation ; autant la variance est petite autant la précision est grande. La liaison entre cette variance et l'information $I(\theta)$ est exprimée par l'inégalité bien connue trouvée indépendamment par Cramer (1946), Darmois (1945), Fréchet (1943) et Rao (1945). Quant à la relation qui existe entre un résumé exhaustif et l'information $I(\theta)$ Fisher y revient à plusieurs reprises, disant qu'un résumé exhaustif contient la totalité de l'information contenue dans un échantillon. La première propriété ne concerne que le problème de l'estimation, mais la seconde peut être considérée comme une propriété générale que doit posséder toute fonction d'information. Nous préciserons cette idée par la suite.

Notons, d'autre part, deux autres propriétés importantes. Premièrement, l'information $I(\theta)$ n'est jamais négative ; on a toujours $I(\theta) \geqslant 0$. Deuxièmement, $I(\theta)$ est additive pour les observations indépendantes ; l'information moyenne contenue dans un échantillon obtenu à partir de n tirages indépendants est égale à $nI(\theta)$.

L'information $I(\theta)$ nous fournit donc un renseignement sur le problème de l'estimation. Si l'on connait $I(\theta)$, on connait la précision que l'on peut atteindre (l'inégalité de Cramer-Darmois-Fréchet-Rao), ce qui permet, par exemple, de juger de l'efficacité d'une méthode d'estimation. Mais l'information $I(\theta)$ perd son importance dès qu'il s'agit d'un problème autre que le problème de l'estimation. Ainsi, il est utile de chercher les fonctions qui pourraient être les fonctions d'information pour d'autres problèmes de statistique mathématique, celui des tests d'hypothèse par exemple. Il devient alors nécessaire de dégager d'abord quelques unes des propriétés générales d'une fonction d'information. Nous le ferons en nous inspirant des propriétés de caractère général que possède l'information $I(\theta)$ de Fisher.

PROPRIETES GENERALES D'UNE FONCTION D'INFORMATION -

Nous prenons comme point de départ un espace mesurable $(X, \mathcal{X})$ sur lequel est définie une famille $\mathcal{M}$ de mesures de probabilité. L'ensemble, $(X, \mathcal{X}, \mathcal{M})$ constitue l'espace d'observations ("sample space"), et toute information sera définie par rapport à cet espace d'observations.

L'information moyenne contenue dans l'espace $(X, \mathcal{X}, \mathcal{M})$ est une fonction numérique bornée :

$$I(\mathcal{M}, X)$$

On peut définir également, si les conditions du problème le permettent, l'information apportée par une observation $x \in X$ comme une fonction de point $i(x;\mathcal{M})$ telle que l'information moyenne $I(\mathcal{M};X)$ s'exprime comme l'intégrale de $i(x;\mathcal{M})$ par rapport à une mesure $\mu \in \mathcal{M}$ convenablement choisie.

La première propriété exigée est que l'information ne soit jamais négative, que l'on ait toujours :

$$I(\mathcal{M}; X) \geqslant 0.$$

On ne demandera pourtant pas que la fonction $i(x;\mathcal{M})$ ait aussi cette propriété. Il est concevable qu'une observation apporte une information négative. Tout ce que l'on demande c'est que l'information moyenne soit non-négative.

La seconde propriété est celle d'additivité. L'information moyenne apportée par n observations indépendantes doit être égale à n fois l'information moyenne d'une seule observation. En langage mathématique si :

$$(X \otimes X, \mathcal{X} \otimes \mathcal{X}, \mathcal{M} \otimes \mathcal{M})$$

est l'espace produit cartésien à deux dimensions de l'espace $(X, \mathscr{X})$, on doit avoir :

$$I(\mathfrak{M} \otimes \mathfrak{M}; X \otimes X) = 2\, I(\mathfrak{M}; X),$$

et de même pour un nombre fini quelconque de dimensions.

La troisième propriété est celle qui concerne le résumé exhaustif. Il y a lieu de préciser le sens de la phrase de Fisher : "un résumé exhaustif contient la totalité de l'information".

Dans le cas général où nous sommes placés, la notion de fonction d'observations ("statistic") est remplacée par celle de transformation mesurable. Si T est une transformation mesurable de l'espace mesurable $(X, \mathscr{X})$ sur un autre espace mesurable $(Y, \mathscr{Y})$, elle définit une famille de mesures de probabilité sur $(Y, \mathscr{Y})$ correspondant à la famille $\mathfrak{M}$. En fait, à toute mesure $\mu \in \mathfrak{M}$ correspond une mesure μT^{-1} sur $(Y, \mathscr{Y})$ définie par :

$$\mu T^{-1}(E) = \mu(F)$$

où on a :

$$E \in \mathscr{Y}, \qquad F = T^{-1}(E).$$

Nous noterons cette nouvelle famille de mesures $\mathfrak{M} T^{-1}$.

On obtient ainsi, par une transformation mesurable T, un nouvel espace d'observations $(Y, \mathscr{Y}, \mathfrak{M} T^{-1})$. L'information associée à ce nouvel espace ne doit pas être supérieure à celle associée à l'espace $(X, \mathscr{X}, \mathfrak{M})$, c'est-à-dire que :

$$I(\mathfrak{M} T^{-1}; Y) \leqslant I(\mathfrak{M}; X).$$

Il est normal d'exiger que l'information possède cette propriété, car une transformation mesurable représente une sorte de groupement des observations antérieures et un tel groupement ne doit pas augmenter l'information. L'information de Fisher a également cette propriété. (Darmois (1936), p. 27 ; Doob (1936), théorème 2).

Ceci dit, nous pouvons maintenant expliciter le rapport entre l'information et le résumé exhaustif. Si la transformation T est un résumé exhaustif, on doit avoir :

$$I(\mathfrak{M} T^{-1}; Y) = I(\mathfrak{M}; X).$$

On pourrait énoncer une condition plus forte à savoir que l'on ait égalité si, et seulement si, la transformation T est un résumé exhaustif. Nous pensons néanmoins que cela n'est pas nécessaire.

Ayant énoncé ces propriétés générales, étudions maintenant deux problèmes particuliers, le problème des tests d'hypothèse et celui de la discrimination.

TESTS D'HYPOTHESE ET INFORMATION -

Supposons que sur l'espace mesurable $(X, \mathcal{X})$ on ait défini deux mesures de probabilité μ et ν qui correspondent respectivement à deux hypothèses, l'hypothèse à tester et l'hypothèse alternative. Selon la théorie de Neyman-Pearson un test de l'hypothèse μ contre l'alternative ν est le choix d'un sous-ensemble R_0 de X, appelé région critique, de telle sorte que l'on rejette l'hypothèse μ toutes les fois que l'observation $x \in X$ se trouve dans R_0. A toute région critique R_0, on associe deux erreurs, l'erreur α du premier type : $\alpha = \mu(R_0)$ et l'erreur β du second type : $\beta = \nu(\bar{R}_0)$,

où $\bar{R}_0$ est l'ensemble complémentaire de R_0. On appelle puissance de test la quantité :

$$1 - \beta = \nu(R_0)$$

Pour une valeur déterminée de α $(0 < \alpha < 1)$, le meilleur test est celui qui rend minima l'erreur du second type ou bien, ce qui est identique, celui qui rend maxima la puissance de test. Il s'agit donc de trouver un sous-ensemble mesurable R_0 de X tel que $\mu(R_0) = \alpha$ et tel que pour tout sous-ensemble mesurable R pour lequel $\mu(R) = \alpha$ on ait $\nu(R_0) \geqslant \nu(R)$.

Supposons que les deux mesures μ et ν soient absolument continues par rapport à une troisième mesure de probabilité λ définie sur le même espace $(X, \mathcal{X})$. Il est toujours possible de trouver une telle mesure ($\lambda = \frac{\mu + \nu}{2}$ par exemple). Désignons par $f(x)$ et $g(x)$ respectivement les dérivées de Radon-Nikodym de μ et de ν par rapport à λ. Il est bien connu que le meilleur test est celui pour lequel la région critique R_0 est l'ensemble des points $x \in X$ tels que :

$$\frac{f(x)}{g(x)} \leqslant k \quad ,$$

k étant choisi de telle sorte que l'on ait $\mu(R_0) = \alpha$.

Nous définissons alors l'information apportée par une observation $x \in X$ comme :

$$i\,(x\,;\,\mu/\nu) = \log \frac{f\,(x)}{g\,(x)}$$

et l'information moyenne comme :

$$\acute{i}\,(\mu/\nu) = \int_X \log \frac{f\,(x)}{g(x)}\, d\mu\,(x) = \int_X f(x) \log \frac{f\,(x)}{g(x)}\, d\lambda\,(x)$$

Nous définissons également l'information contenue dans un sous-ensemble mesurable $E \in \mathscr{X}$ comme :

$$I_E\,(\mu/\nu) = \frac{1}{\mu\,(E)} \int_E f(x) \log \frac{f\,(x)}{g\,(x)}\, d\lambda\,(x)$$

Ces définitions sont dues à Kullback et Leibler qui ont aussi démontré que la fonction $I(\mu/\nu)$ possède toutes les propriétés générales d'une information que nous venons d'énoncer. Ils l'appellent information de discrimination entre μ et ν. Nous préférons plutôt l'appeler information de test de l'hypothèse μ contre ν. Et ceci pour deux raisons : d'abord parce que la fonction $I(\mu/\nu)$ n'est pas symétrique par rapport à μ et ν ; ensuite à cause de la liaison qui existe entre $I(\mu/\nu)$ et la méthode de Neyman-Pearson, liaison que nous allons établir dans ce qui suit.

Soit R_o la région définit plus haut. On voit facilement que, pour tout sous-ensemble mesurable $R \in \mathscr{X}$ pour lequel $\mu(R) = \alpha$ on a :

$$I_R\,(\mu/\nu) \geqslant I_{R_o}\,(\mu/\nu)$$

De même :

$$I_{\bar{R}}\,(\mu/\nu) \leqslant I_{\bar{R}_o}\,(\mu/\nu)\,,$$

$\bar{R}$ et $\bar{R}_o$ étant respectivement les ensembles complémentaires de R et de R_o. La méthode de Neyman-Pearson équivaut ainsi à choisir parmi toutes les régions critiques celle qui englobe le minimum d'information ou bien de choisir parmi toutes les régions d'acceptation celle qui englobe le maximum d'information.

Considérons maintenant l'espace produit cartésien $(U, \mathscr{U})$ à n dimensions de l'espace $(X, \mathscr{X})$. Désignons par L, M et N les mesures produites correspondant respectivement à λ, μ et ν. Les mesures M et N sont absolument continues par rapport à la mesure L, et si l'on désigne par $\Phi(u)$, $\Psi(u)$ les dérivées de Radon-Nikodym, on a :

$$\phi\,(u) = f(x_1)\,f(x_2)\,\ldots\,f(x_n)$$

$$\Psi\,(u) = g(x_1)\,g(x_2)\,\ldots\,g(x_n)$$

où :

$$u = (x_1,\ x_2,\ \ldots\ ,\ x_n)\ .$$

L'additivité de l'information nous donne :

$$I(M/N) = \int_U \log\frac{\Phi(u)}{\Psi(u)}\,dM\,(u) = n\int_X \log\frac{f(x)}{g(x)}\,d\,\mu(x) = nI(\mu/\nu)$$

Ainsi, d'après la loi des grands nombres, étant donnés ε et δ deux nombres positifs arbitrairement petits, on peut trouver un nombre entier $n_0(\varepsilon, \delta)$ tel que pour tout nombre $n \geqslant n_0$ on ait :

$$M\left\{u :\ \left|\frac{1}{n}\log\frac{\Phi(u)}{\Psi(u)} - I\,(\mu/\nu)\right| < \varepsilon\right\} > 1 - \delta\ .$$

L'espace U se décompose ainsi en deux sous-ensembles W et $\overline{W}$ (ensemble complémentaire) tels que l'on ait :

$$M(W) > 1 - \delta\ ,$$

et tels que pour tout point $u \in W$ on ait :

$$e^{n\,[I(\mu/\nu)-\epsilon]} < \frac{\Phi\,(u)}{\Psi\,(u)} < e^{n\,[I(\mu/\nu)+\epsilon]}$$

d'où (cf. chap. III, théorème 7) :

$$(1-\delta)\,e^{-n\,[I(\mu/\nu)+\epsilon]} < N(W) < e^{-n\,[I(\mu/\nu)-\epsilon]}$$

On pourrait alors prendre le sous-ensemble $\overline{W}$ comme région critique et on aurait :

$$M(\overline{W}) < \delta\ ,\ N(\overline{W}) > 1 - e^{-n\,[I(\mu/\nu)-\epsilon]}$$

Ainsi on voit que lorsque le nombre d'observations augmente, l'erreur du premier type tend vers zéro tandis que la puissance de test tend vers l'unité. De plus on a :

$$I_W\,(M\,|\,N) = \frac{1}{M\,(W)}\int_W \log\frac{\Phi(u)}{\Psi(u)}\,dM\,(u)\ ,$$

et donc :

$$n [I(\mu/\nu) - \varepsilon] < I_w(M/N) < n [I(\mu/\nu) + \varepsilon]$$

ce qui montre qu'à la limite le sous-ensemble W (région d'acceptation) contient à peu près la totalité de l'information I(M/N).

L'importance de l'information $I(\mu/\nu)$ pour les tests d'hypothèse est encore mieux révélée par le théorème suivant qui généralise un résultat de Shannon ((1948), théorème 4). Ce théorème nous permet de démontrer que pour toute valeur fixée de l'erreur α du premier type l'erreur β du second type tend exponentiellement vers zéro lorsque ce nombre d'observations augmente et que cette décroissance dépend de l'information $I(\mu/\nu)$. Bien entendu, ceci n'est vrai que si l'on emploie le meilleur test au sens de la théorie de Neyman-Pearson.

THEOREME 1 :

Soit a un nombre arbitraire compris entre 0 et 1 ($0 < a < 1$). Soit W_a et $\overline{W}_a$ (l'ensemble complémentaire de W_a) deux sous-ensembles de l'espace U tels que :

$$\frac{\Phi(u_1)}{\Psi(u_1)} > \frac{\Phi(u_2)}{\Psi(u_2)}$$

pour tout point $u_1 \in W_a$ et $u_2 \in \overline{W}_a$. Si $M(W_a) = a$, on a pour n suffisamment grand :

$$(a - \delta)\, e^{-n[I(\mu/\nu)+\epsilon]} < N(W_a) < e^{-n[I(\mu/\nu)-\epsilon]}$$

où ε et δ sont deux nombres positifs arbitrairement petits qui tendent vers zéro lorsque n tend vers l'infini.

Nous avons déjà vu que pour n suffisamment grand l'espace U se décompose en deux sous-ensembles W et $\overline{W}$ tel que l'on ait :

$$e^{n[I(\mu/\nu)-\epsilon]} < \frac{\Phi(u)}{\Psi(u)} < e^{n[I(\mu/\nu)+\epsilon]}$$

pour tout point $u \in W$, et tel que $M(W) > 1 - \delta$.

Le sous-ensemble W_a contient évidemment tous les points u pour lesquels :

$$\frac{\Phi(u)}{\Psi(u)} \geqslant e^{n[I(\mu/\nu)+\epsilon]}$$

Il contient aussi une partie du sous-ensemble W. Les points u pour lesquels :

$$\frac{\Phi(u)}{\Psi(u)} \leqslant e^{n[I(\mu/\nu)-\epsilon]}$$

ne font pas partie de W_a. Ainsi pour tout point $u \in W_a$ on a :

$$\frac{\Phi(u)}{\Psi(u)} > e^{n[I(\mu/\nu)-\epsilon]}$$

ce qui donne :

$$\int_{W_a} \frac{\Phi(u)}{\Psi(u)} dN(u) > N(W_a)\, e^{n[I(\mu/\nu)-\epsilon]}$$

c'est-à-dire :

$$M(W_a) > N(W_a)\, e^{n[I(\mu/\nu)-\epsilon]}$$

Comme $M(W_a) \leqslant 1$, on a :

$$N(W_a) < e^{-n[I(\mu/\nu)-\epsilon]}$$

ce qui démontre une partie du théorème.

Désignons par S_a l'ensemble des points u appartenant à la partie commune de W_a et W. Ainsi pour tout point $u \in S_a$ on a :

$$\frac{\Phi(u)}{\Psi(u)} < e^{n[I(\mu/\nu)+\epsilon]}$$

On a donc :

$$M(S_a) = \int_{S_a} \frac{\Phi(u)}{\Psi(u)} dN(u) < N(S_a)\, e^{n[I(\mu/\nu)+\epsilon]}$$

Mais :

$$M(S_a) + M(W_a - S_a) = M(W_a) = a$$

et :

$$M(W_a - S_a) < \delta \ .$$

On a ainsi :

$$M(S_a) > a - \delta$$

D'autre part :

$$N(S_a) < N(W_a)$$

ce qui donne finalement :

$$(a - \delta) < N(W_a)\, e^{n[I(\mu/\nu)+\epsilon]}$$

ou :

$$N(W_a) > (a - \delta)\, e^{-n[I(\mu/\nu)+\epsilon]}$$

et le théorème est complètement démontré.

Pour revenir au problème du test d'hypothèse remarquons qu'au lieu de choisir dans l'espace U une région critique de "taille" α (erreur du premier type) on peut choisir une région d'acceptation d'un seuil de confiance $a = 1 - \alpha$. On voit que le meilleur test selon la théorie de Neyman-Pearson conduirait à la même décomposition de l'espace U que celle considérée ci-dessus. Le sous-ensemble $W_a (a = 1 - \alpha)$ est la région d'acceptation et nous voyons que l'erreur du second type, c'est-à-dire $N(W_a)$, tend vers zéro avec n, plus précisément :

$$N(W_a) < e^{-n[I(\mu/\nu)-\epsilon]}$$

Tous ces résultats ne sont valables que si l'intégrale qui définit l'information existe. Or il est facile de trouver des exemples où cette intégrale est infinie. Il se peut aussi que des deux informations $I(\mu/\nu)$ et $I(\nu/\mu)$, l'une soit finie et l'autre infinie. Ceci est montré par l'exemple suivant que nous a communiqué Schutzenberger.

Soient :

$$K = \sum_{n=2}^{\infty} \frac{1}{n(\log n)^2} < \infty$$

$$K' = \sum_{n=2}^{\infty} \frac{1}{n^2(\log n)^2} < \infty$$

Considérons deux lois de probabilité :

$$P : \left\{ p_n = \frac{K^{-1}}{n(\log n)^2} \quad , \quad n = 2, 3, \ldots \right\}$$

$$P' : \left\{ p_n = \frac{K'^{-1}}{n^2(\log n)^2} \quad , \quad n = 2, 3, \ldots \right\}$$

On a :

$$I(P/P') = \sum_{n=2}^{\infty} P_n \log \frac{P_n}{P'_n}$$

$$= \sum_{n=2}^{\infty} \frac{K^{-1}}{n(\log n)^2} \operatorname{Log} \frac{K'}{K} \cdot n$$

$$\sim \sum \frac{1}{n \log n} > \infty$$

et :

$$I(P'/P) = \sum_{n=2}^{\infty} P'_n \log \frac{P'_n}{P_n}$$

$$= \sum_{n=2}^{\infty} \frac{K'^{-1}}{n^2(\log n)^2} \log \frac{K}{K'} \cdot \frac{1}{n}$$

$$\sim \sum \frac{1}{n^2 \log n} < \infty$$

INFORMATION ET PROBLEME DE DISCRIMINATION -

Considérons le problème de discrimination entre deux mesures de probabilité μ et ν définies sur un même espace mesurable $(X, \mathfrak{X})$. D'après Welch (1939) il s'agit de décomposer l'espace X en deux sous-ensembles mesurables disjoints R_μ et R_ν $(R_\mu \cup R_\nu = X)$ appelés respectivement région d'acceptation de μ et de ν. Si l'observation $x \in X$ se trouve dans R_μ on accepte la mesure μ, sinon on accepte la mesure ν Cette décomposition doit être faite suivant un critère donné d'optimalité. On peut, par exemple, choisir parmi toutes les décompositions celle qui rend minima l'erreur totale c'est-à-dire la quantité :

$$\mu(R_\nu) + \nu(R_\mu) \;;$$

ou bien choisir parmi les décompositions telles que :

$$\mu(R_\nu) = \nu(R_\mu)$$

celle qui rend minima cette quantité (l'erreur commune). Nous prenprendrons comme critère la réduction d'une fonction linéaire des erreurs. C'est-à-dire que la décomposition choisie sera celle qui rend minima la quantité :

$$\gamma = \alpha \mu (R_\nu) + \beta \nu (R_\mu)$$

où α et β sont deux nombres positifs déterminés. $(\alpha + \beta = 1)$.

Supposons toujours que les mesures μ et ν soient absolument continues par rapport à une troisième mesure de probabilité λ définie également sur $(X, \mathscr{X})$, et désignons par $f_\mu(x)$ et $f_\nu(x)$ les dérivées de Radon-Nikodym correspondantes. Nous définissons alors l'information de discrimination comme :

$$I(\mu, \nu) = -\log \left[\inf_{o<t<1} \int_X [(f_\mu(x))^t (f_\nu(x))^{1-t}] \, d\lambda(x)\right.$$

$I(\mu, \nu)$ est la fonction proposée par Chernoff (1952) comme une mesure de divergence entre deux lois de probabilité.

Nous démontrerons d'abord que la fonction $I(\mu, \nu)$ possède les propriétés générales d'une information. Désignons par $\rho(t)$ la quantité

$$\rho(t) = \int_X [f_\mu(x)]^t \, [f_\nu(x)]^{1-t} \, d\lambda(x), \quad 0 < t < 1.$$

$\rho(t)$ peut être considérée comme une généralisation de la fonction d'affinité de Bhattacharya (1943) qui mesure, en quelque sorte, combien μ et ν sont proches l'une de l'autre. Posons ensuite $\rho = \inf_{o<t<1} \rho(t)$. On a ainsi $I(\mu, \nu) = -\log \rho$.

L'inégalité de Holder nous donne les lemmes suivants :

Lemme 1 :

$$0 \leqslant \rho(t) \leqslant 1.$$

Lemme 2 :

Pour tout sous-ensemble mesurable $E \in \mathscr{X}$ on a :

$$\int_E [f_\mu(x)]^t \, [f_\nu(x)]^{1-t} \, d\lambda(x) < [\mu(E)]^t \, [\nu(E)]^{1-t}$$

Une transformation mesurable T de $(X, \mathscr{X})$ sur un autre espace mesurable $(Y, \mathscr{Y})$ définit sur $(Y, \mathscr{Y})$ les mesures de probabilité μT^{-1}, νT^{-1} et λT^{-1} correspondant respectivement à μ, ν et λ définies sur $(X, \mathscr{X})$. Les mesures μT^{-1}, νT^{-1} sont absolument continues par rapport à la mesure λT^{-1}. Désignons par $g_\mu(y)$, $g_\nu(y)$ les dérivées de Radon-Nikodym correspondantes. La fonction $\rho(t)$ définie par rapport à l'espace $(X, \mathscr{X})$ se remplace alors par la fonction $\rho_T(t)$ définie sur l'espace $(Y, \mathscr{Y})$. On a :

$$\rho_T(t) = \int_Y [g_\mu(y)]^t \, [g_\nu(y)]^{1-t} \, d\lambda T^{-1}(y).$$

THEOREME 2 :

Pour toute transformation mesurable T de $(X, \mathcal{X})$ sur $(Y, \mathcal{Y})$ on a :

$$\rho_T(t) \geqslant \rho(t)$$

On peut toujours écrire :

$$\rho(t) = \int_X \left[\frac{f_\mu(x)}{f_\nu(x)} \right]^t d\nu(x)$$

$$\rho_T(t) = \int_Y \left[\frac{g_\mu(y)}{g_\nu(y)} \right]^t d\nu T^{-1}(y) .$$

D'après un résultat bien connu (Halmos (1954), théorème 39 c) on a :

$$\rho_T(t) = \int_X \left[\frac{g_\mu T(x)}{g_\nu T(x)} \right]^t d\nu(x)$$

où $g_\mu T(x)$ et $g_\nu T(x)$ sont deux fonctions mesurables $(T^{-1}(\mathcal{Y}))$ définies sur X à partir des fonctions $g_\mu(y)$ et $g_\nu(y)$ définies sur Y (voir Halmos (1954), p. 162). Mettons :

$$g(x) = \frac{g_\mu T(x)}{g_\nu T(x)}$$

et soit $G_k^{(n)}$ l'ensemble :

$$G_k^{(n)} = \left\{ x : \frac{k}{2^n} < [g(x)]^t \leqslant \frac{k+1}{2^n} \right\} \quad , k = 0, 1, 2, \ldots$$

Alors :

$$G_k^{(n)} \in T^{-1}(\mathcal{Y}), \bigcup_k G_k^{(n)} = X .$$

Soit :

$$S_n = \sum_{k=0}^{\infty} \frac{k}{2^n} \nu(G_k^{(n)})$$

alors :

$$\lim_{n \to \infty} S_n = \int_X [g(x)]^t \, d\nu(x).$$

Or, pour $x \in G_k^{(n)}$, on a :

$$\left(\frac{k}{2^n}\right)^{\frac{1}{t}} < g(x) \leqslant \left(\frac{k+1}{2^n}\right)^{\frac{1}{t}}$$

Donc :

$$\left(\frac{k}{2^n}\right)^{\frac{1}{t}} \nu(G_k^{(n)}) < \int_{G_k^{(n)}} g(x)\, d\nu(x) \leqslant \left(\frac{k+1}{2^n}\right)^{\frac{1}{t}} \nu(G_k^{(n)})$$

c'est-à-dire :

$$\left(\frac{k}{2^n}\right)^{\frac{1}{t}} < \frac{\mu(G_k^{(n)})}{\nu(G_k^{(n)})} \leqslant \left(\frac{k+1}{2^n}\right)^{\frac{1}{t}}$$

ou :

$$\frac{k}{2^n} < \left[\frac{\mu(G_k^{(n)})}{\nu(G_k^{(n)})}\right]^t \leqslant \frac{k+1}{2^n}$$

On a ainsi :

$$\int_X [\, g(x)\,]^t \, d\nu(x) = \lim_{n\to\infty} S_n$$

$$= \lim_{n\to\infty} \sum_{k=o}^{\infty} [\, \mu(G_k^{(n)})\,]^t \, [\nu(G_k^{(n)})\,]^{1-t}$$

Mais, d'après le lemme 2,

$$\rho(t) = \int_X [\, f_\mu(x)\,]^t \, [f_\nu(x)\,]^{1-t} d\lambda(x) = \sum_{k=o}^{\infty} \int_{G_k^{(n)}} (f_\mu(x)^t f_\nu(x)^{1-t} d\lambda(x)$$

$$\leqslant \lim_{n\to\infty} \sum_{k=o}^{\infty} [\, \mu(G_k^{(n)}\,]^t \, [\nu(G_k^{(n)})\,]^{1-t} = \rho_T(t)$$

Le théorème est donc démontré.

D'après Halmos et Savage (1949) si la transformation T est un résumé exhaustif pour une classe $\mathcal{M}$ de mesures de probabilité définies sur $(X, \mathcal{X})$, on a :

$$f_\mu(x) = g_\mu T(x)$$

pour toute mesure $\mu \in \mathcal{M}$ sauf sur un ensemble de λ-mesure nulle. Ainsi on voit facilement que si la transformation T est un résumé exhaustif, on a :

$$\rho_T(t) = \rho(t)$$

Soient $\mu \otimes \mu$; $\nu \otimes \nu$ les mesures produites définies sur l'espace produit cartésien $(X \otimes X, \mathcal{X} \otimes \mathcal{X})$. Si l'on désigne par $\rho^{(2)}(t)$ la fonction correspondant à $\rho(t)$, on a évidemment :

$$\rho^{(2)}(t) = [\, \rho(t)\,]^2$$

A partir de ces propriétés de la fonction $\rho(t)$, on déduit facile-

ment que la fonction $I(\mu, \nu)$ possède toutes les propriétés générales d'une information. On a ainsi :

1/ - $I(\mu, \nu) \geqslant 0$, avec égalité si, et seulement si, les mesures μ et ν sont identiques.

2/ - $I(\mu, \nu) < +\infty$, sauf dans le cas où $\mu \perp \nu$.

3/ - $I(\mu \otimes \mu, \nu \otimes \nu) = 2\, I(\mu, \nu)$.

4/ - $I(\mu, \nu)$ n'augmente pas sous les transformations mesurables et reste invariant si la transformation est un résumé exhaustif.

Ajoutons à cela la propriété de symétrie, on a :

$$I(\mu, \nu) = I(\nu, \mu).$$

Revenons maintenant au problème principal : pourquoi nous appelons la fonction :

$$I(\mu, \nu) = -\log \rho$$

information de discrimination entre μ et ν. Nous avions choisi comme critère d'optimalité la minimisation de la quantité :

$$\gamma = \alpha\, \mu(R_\nu) + \beta\, \nu(R_\mu), \quad (\alpha + \beta = 1).$$

α et β étant deux nombres positifs donnés. Il est bien connu que la décomposition optimale est celle définie par :

$$R_\mu = \{ x : \quad \alpha\, f_\mu(x) \geqslant \beta\, f_\nu(x) \}$$

$$R_\nu = \{ x : \quad \alpha\, f_\mu(x) \leqslant \beta\, f_\nu(x) \}$$

Nous avons alors, pour une telle décomposition de l'espace $(X, \mathscr{X})$ le théorème suivant :

THEOREME 3 :

$$\gamma \leqslant 2\rho$$

On peut toujours écrire :

$$\rho(t) = \int_X \left[\frac{f_\mu(x)}{f_\nu(x)}\right]^t d\nu(x) = \int_X \left[\frac{f_\nu(x)}{f_\mu(x)}\right]^{1-t} d\mu(x)$$

On obtient ainsi :

$$\rho\ (t) \geqslant \int_{R_\mu} [\frac{f_\mu(x)}{f_\nu(x)}]^t \ d\nu(x) \geqslant (\frac{\beta}{\alpha})^t \ \nu(R_\mu)$$

De même on a :

$$\rho\ (t) \geqslant \int_{R_\nu} [\frac{f_\nu(x)}{f_\mu(x)}]^{1-t} \ d\mu\ (x) \geqslant (\frac{\alpha}{\beta})^{1-t} \ \mu(R_\nu)$$

Il en résulte que :

$$\begin{aligned} \gamma &= \alpha\ \mu\ (R_\nu) + \beta\ \nu\ (R_\mu) \\ &\leqslant [\alpha . (\frac{\beta}{\alpha})^{1-t} + \beta\ .\ (\frac{\alpha}{\beta})^t\ ]\ \rho\ (t) \\ &= 2\ \alpha^t\ \beta^{1-t}\ \rho\ (t) \\ &\leqslant 2\ \rho\ (t) \end{aligned}$$

c'est-à-dire que :

$$\gamma \leqslant 2\ \rho$$

Remarquons que si l'on prend $\alpha = \beta = \frac{1}{2}$ on obtient $\gamma \leqslant \rho$

Pour un nombre n d'observations indépendantes on a donc :

$$\gamma \leqslant 2\ \rho^n \ = 2\ e^{-n I(\mu,\nu)} \leqslant \ e^{-n [I(\mu,\nu)-\epsilon]}$$

où $\varepsilon \longrightarrow 0$, lorsque $n \longrightarrow \infty$. Ainsi, à la limite, l'erreur γ tend exponentiellement vers zéro avec $I(\mu,\ \nu)$. Par conséquent, la fonction $I(\mu,\ \nu)$ peut bien être considérée comme information de discrimination entre μ et ν.

L'information de discrimination possède des propriétés semblables à celles d'une mesure de "divergence" ou "distance" entre deux lois de probabilité. (Pour les détails sur les différentes "distances" voir Adhikari et Joshi (1956)). Ce qui distingue l'information de la distance c'est la propriété d'additivité. L'information est additive pour les espaces produits tandis que la distance est une fonction croissante sans être nécessairement additive. Par contre, s'il est souhaitable que la distance satisfasse à l'inégalité triangulaire, il n'est pas nécessaire que l'information ait aussi cette propriété. Les considérations suivantes montrent qu'en général ces deux propriétés sont incompatibles au moins si l'on veut que la distance et l'information gardent un sens pour le problème de la discrimination.

Supposons que l'on ait une fonction $I(\mu, \nu)$ définie pour tout couple de mesures μ et ν et ayant les propriétés suivantes :

(i) $I(\mu, \nu) = I(\nu, \mu)$

(ii) $I(\mu, \nu) > 0$

(iii) $I(\mu, \mu) = 0$

Ces propriétés sont communes à l'information et à la distance. La discrimination entre deux mesures singulières se faisant toujours sans erreur il est normal d'exiger que la fonction $I(\mu, \nu)$ ait la plus grande valeur dans le cas où $\mu \perp \nu$. Supposons maintenant que la fonction $I(\mu, \nu)$ soit additive, c'est-à-dire que l'on ait :

$$I(\mu \otimes \mu, \nu \otimes \nu) = 2\, I(\mu, \nu)$$

La propriété d'additivité entraîne ainsi l'existence des valeurs infinies et l'on doit poser :

$$I(\mu, \nu) = \infty \text{ pour } \mu \perp \nu.$$

Si l'on suppose maintenant que la fonction $I(\mu, \nu)$ reste finie dans tous les autres cas on voit facilement que l'inégalité triangulaire ne peut pas être satisfaite. Prenons deux mesures singulières μ et ν et une troisième mesure λ ($= \frac{\mu + \nu}{2}$ par exemple) qui n'est pas singulière ni par rapport à μ ni par rapport ν. On a donc :

$$I(\mu, \lambda) < \infty, \quad I(\nu, \lambda) < \infty$$

et :

$$I(\mu, \nu) = \infty$$

c'est-à-dire :

$$I(\mu, \lambda) + I(\lambda, \nu) < I(\mu, \nu).$$

BIBLIOGRAPHIE

1 - B.P. ADHIKARI (1957) - C. R. Acad. Sc. Paris, 244, p. 1 000.

2 - B. P. ADHIKARI & D. D. JOSHI (1956) - Publ. Inst. Stat. Univ. Paris, 5, p. 57.

3 - G. A. BARNARD (1951) - Journ. Roy. Stat. Soc., 13, p. 46.

4 - A. BHATTACHARYA (1943) - Bull. Cal. Math. Soc., 35, p. 99.

5 - H. CHERNOFF (1952) - Ann. Math. Stat., 23, p. 493.

6 - H. CRAMER (1946) - Mathematical Methods of Statistics, Princeton.

7 - G. DARMOIS (1936) - Méthodes d'Estimation, Act. Sc. Ind., n°356, Paris.

8 - G. DARMOIS (1945) - Rev. Inst. Int. Stat., 13, p. 9.

9 - J. L. DOOB (1953) - Stochastic Processes, New-York.

10 - J. L. DOOB (1936) - Trans. Amer. Math. Soc., 39, p. 410.

11 - A. FEINSTEIN (1954) - Trans. I.R.E. PGIT-4, P. 2.

12 - R. FORTET (1951) - La Cybernétique (Réunions Louis de Broglie), Paris p. 9.

13 - M. FRÉCHET (1943) - Rev. Inst. Int. Stat., 11, p. 183.

14 - A. & D. GABOR (1954) - Journ. Roy. Stat. Soc., Série A, 117, p. 31.

15 - E. N. GILBERT (1952) - Bell Sys. Techn. Journ., 31, p. 504.

16 - P. R. HALMOS (1954) - Measure Theory, New York.

17 - P. R. HALMOS & L. J. SAVAGE (1949) - Ann. Math. Stat., 20, p. 225.

18 - R. W. HAMMING (1950) - Bell Sys. Techn. Journ., 29, p. 147.

19 - G. H. HARDY, J. E. LITTLEWOOD & G. POLYA (1934) - Inequalities, Cambridge.

20 - A. KHINTCHINE (1953) - Yspekhi. Matem. Nauk., 8, 3(55), p. 3.

21 - A. KHINTCHINE (1956) - Yspekhi. Matem. Nauk., 11, 1(67), p. 17.

22 - Y. KOMAMIYA (1954) - Proc. 3rd (1953) Japan Nat. Cong. App. Math., p. 437.

23 - S. KULLBACK & R. A. LEIBLER (1951) - Ann. Math. Stat., 22, p. 79.

24 - A. E. LAEMMEL (1952) - Symp. Comm. Th., London, p. 102.

25 - B. Mc MILLAN (1953) - Ann. Math. Stat., 24, p. 196.

26 - D. E. MULLER (1953) - Rep. N°46, Digital Computer Laboratory, University of Illinois, Urbana.

27 - D. E. MULLER (1954) - I. R. E. Tans. On Electronic Computers,

28 - J. NEYMAN & E. S. PEARSON (1952) - Phil. Trans. A., 231, p.289.

29 - C. R. RAO (1945) - Bull. Cal. Math. Soc., 37, p. 81.

30 - I. S. REED (1953) - Techn. Rep. N°44. Lincoln Laboratory, M. I. T.

31 - H. ROBBINS (1948) - Ann. Math. Stat., 19, p. 360.

32 - S. SAKS (1937) - The Theory of the Integral, New York.

33 - M. P. SCHUTZENBERGER (1953) - Publ. Inst. Stat. Univ. Paris, 2, p. 125.

34 - M. P. SCHUTZENBERGER (1954) - Publ. Inst. Stat. Univ. Paris, 3, p. 3.

35 - C. E. SHANNON (1948) - Bell. Sys. Techn. Journ., 27, p. 379 et p. 623.

36 - D. SLEPIAN (1956) - Bell. Sys. Techn. Journ., 35, p. 203.

37 - B. L. WELCH (1939) - Biometrika, 31, p. 218.

38 - N. WIENER (1948) - Cybernetics, New York.

39 - S.K. ZAREMBA (1952) - Journ. Lond. Math. Soc., 27, p. 242.

TABLE DES MATIÈRES

Pages

INTRODUCTION 83

CHAPITRE I -
Le théorème fondamental de la théorie de l'information : cas discret 87

CHAPITRE II -
Le problème du codage binaire 101

CHAPITRE III -
Le théorème fondamental : cas général 119

CHAPITRE IV -
L'information en statistique mathématique 141

SUR L'INÉGALITÉ DE SLUTSKY

A. FUCHS

L'objet de la présente note est de donner une démonstration très simple de l'inégalité entre moments connue sous le nom d'inégalité de Slutsky [1] et de la comparer à d'autres inégalités analogues.

Lemme 1.

Pour $x, y > 0$; $p, q > 0$, $p + q = 1$ on a :

$$x^p y^q \leqslant p^p q^q (x + y) \tag{1}$$

On remarque que (1) peut s'écrire :

$$\left(\frac{x}{x+y}\right)^p \left(\frac{y}{x+y}\right)^q \leqslant p^p q^q ;$$

il en résulte qu'il suffit de démontrer (1) pour $x+y = 1$, c'est-à-dire, en définitive, de démontrer $x^p y^q < p^p q^q$ pour $x, y > 0$, $x + y = 1$; $p, q > 0$, $p + q = 1$. Mais cette dernière inégalité est évidente puisque :

$$x^p y^q = x^p (1-x)^q \leqslant \underset{x \in [0,1]}{\mathrm{Max}} \; x^p (1-x)^q = p^p q^q$$

Inégalité de Slutsky.

Soient X et Y deux variables aléatoires définies sur une même catégorie d'épreuves. Pour $r, s > 0$ et si $E\{|X|^{r+s}\} < \infty$, $E\{|Y|^{r+s}\} < \infty$ on a :

$$E\{|X|^r |Y|^s\} \leqslant \left(\frac{r}{r+s}\right)^{\frac{r}{r+s}} \left(\frac{s}{r+s}\right)^{\frac{s}{r+s}} \left(E\{|X|^{r+s}\} + E\{|Y|^{r+s}\}\right) \tag{2}$$

Appliquons en effet (1) à $|X|$ et $|Y|$; pour chaque épreuve il vient :

$$|X|^p |Y|^q \leqslant p^p q^q (|X| + |Y|)$$

d'où, en supposant $E\{|X|\} < \infty$, $E\{|Y|\} < \infty$:

$$E\{|X|^p\ |Y|^q\} \leqslant p^p q^q\,(E\{|X|\} + E\{|Y|\}) \qquad (2')$$

Remplaçons alors $|X|$ par $|X|^{r+s}$, $|Y|$ par $|Y|^{r+s}$, posons $p = \frac{r}{r+s}$, $q = \frac{s}{r+s}$ et supposons $E\{|X|^{r+s}\} < \infty$, $E\{|Y|^{r+s}\} < \infty$, (2') est transformé en (2) qui se trouve ainsi établie.

Lemme 2

Pour $x, y > 0$; $p, q > 0$, $p + q = 1$, on a :

$$x^p y^q \leqslant px + qy \qquad (3)$$

C'est l'inégalité classique entre moyennes arithmétique et géométrique. Remarquons que si l'on essaie de majorer le second membre de (3) par une quantité faisant intervenir la somme $x + y$ on obtient $px + qy \leqslant \text{Max}(p, q)\ (x + y)$. Mais comme $p^p q^q \leqslant \text{Max}(p, q)$, l'inégalité ainsi obtenue serait en général plus faible que (1) ; aussi nous tiendrons-nous à l'inégalité (3).

En opérant comme ci-dessus et en supposant toujours, $E\{|X|^{r+s}\} < \infty$, $E\{|Y|^{r+s}\} < \infty$, pour $r, s > 0$ on en déduit l'inégalité :

$$E\{|X|^r\ |Y|^s\} \leqslant \frac{r}{r+s}\ E\{|X|^{r+s}\} + \frac{s}{r+s}\ E\{|Y|^{r+s}\} \qquad (4)$$

analogue à (2) et qui s'y réduit pour $r = s$.

Comparaison des inégalités (2) et (4).

Essayons de comparer les inégalités (2) et (4) ou, ce qui revient au même, les inégalités (1) et (3). A cet effet il suffira de comparer les deux quantités $p^p q^q$ et $px + qy$ pour $x + y = 1$, c'est-à-dire les deux quantités $p^p q^q$ et $px + q(1-x) = q + (p-q)\,x$ pour $x \in [0, 1]$.

Nous excluons le cas $p = q$, pour lequel les inégalités (1) et (3) coïncident. Lorsque $p \neq q$ nous pouvons toujours, sans perte de généralité, supposer $p > q$; il suffirait, le cas échéant, d'échanger les rôles de x et de y.

Une simple étude de la fonction (de p) $y = p^p (1-p)^{1-p}$, $p \in]0, 1[$ montre que $\text{Min}(p, q) \leqslant \frac{1}{2} \leqslant p^p q^q \leqslant \text{Max}(p, q)$, c'est-à-dire, dans notre cas, $q \leqslant \frac{1}{2} \leqslant p^p q^q \leqslant p$. Ceci entraîne que la parallèle $y = p^p q^q$ à Ox

coupe le segment de droite $y = q + (p-q)\, x$, $x \in [0, 1]$ en un point d'abscisse $\alpha \in [0, 1]$ tel que :

$$q + (p-q)\,\alpha = p^p q^q \Rightarrow \alpha = \frac{p^p q^q - q}{p - q}$$

Puisque $\frac{1}{2} \leqslant p^p q^q \leqslant 1$, on a d'ailleurs $\frac{1}{2} \leqslant \alpha \leqslant 1$.

Nous avons alors $q + (p-q)\, x \leqslant p^p q^q$ pour $0 \leqslant x \leqslant \alpha$. Il en résulte, toujours dans l'hypothèse $p > q$, que (3) est plus stricte que (1) lorsque $x < \alpha\,(x + y)$ et que c'est le contraire lorsque $x > \alpha\,(x + y)$.

On en déduit immédiatement :

THEOREME -

Supposons $r > s$ et posons :

$$\alpha = \frac{r^{\frac{r}{r+s}}\, s^{\frac{s}{r+s}} - s}{r - s}$$

Alors (4) est plus stricte que (2) lorsque $E\{|X|^{r+s}\} < \alpha\, E\{|X|^{r+s} + |Y|^{r+s}\}$; c'est le contraire losque $E\{|X|^{r+s}\} > \alpha\, E\,\{|X|^{r+s} + |Y|^{r+s}\}$.

REFERENCE

(1) - M. FRECHET - Recherches théoriques modernes sur le Calcul des Probabilités ; t. I. (1950) Gauthiers-Villars ; p. 66. Signalons en passant une erreur dans le texte ; la quantité désignée à la p. 66 par $k(r, s)$ n'est pas $\leqslant \frac{1}{2}$, mais on a $\frac{1}{2} \leqslant k(r, s) \leqslant 1$.

ANALYSE D'OUVRAGES

Probabilités, Statistique, Recherche Opérationnelle
Collection dirigée Par Georges DARMOIS, Membre de l'Institut

Section A : Théorie des Probabilités

ENSEMBLES MESURABLES
ET
PROBABILISABLES

La Mesure des Ensembles linéaires
la raréfaction des Ensembles de mesure nulle

Par D. DUGUÉ
Professeur à la Sorbonne

Rédigé par M. BARBUT et R. JANIN
-Dunod 1958 -
Analysé par M. BARBUT

Dans un exposé entièrement autonome, l'auteur présente la théorie de la mesure sur la droite, telle qu'E. Borel et H. Lebesgue l'ont conçue.

Les notions fondamentales relatives aux ensembles linéaires étant rappelées, le schéma de l'exposé est le suivant :

Un ensemble est mesurable au sens de Borel, s'il est obtenu à partir d'une infinité dénombrable d'opérations réunion et intersection portant sur des intervalles ouverts. Les ouverts appartiennent à cette classe et la mesure d'un tel ensemble est le résultat des opérations correspondantes d'addition et de soustraction sur les longueurs des intervalles ;

Un ensemble est de mesure nulle s'il peut être enfermé dans des intervalles de longueur totale arbitrairement petite.

Les ensembles mesurables -L sont alors tels que mesures extérieure et intérieure coïncident ; ils sont d'ailleurs réunion d'un ensemble mesurable -B et d'un ensemble de mesure nulle.

Les ensembles mesurables-L forment un σ-corps et leur mesure est dénombrablement additive, on en déduit la monotonie et la continuité.

Une fonction f sur (0,1) est mesurable si, quel que soit y, l'ensemble des points $(x : f(x) < y)$ est mesurable -L.

Si f est bornée on définit son intégrale de Lebesgue par $\int y dg(y)$ (Riemann-Stieltjes), où $g(y) = \text{mes.} (x : f(x) < y)$.

On a, alors, les théorèmes d'Egoroff et de Lebesgue. Enfin, on étend, comme pour l'intégrale de Riemann, la définition aux fonctions sommables.

Le chapitre se termine par l'exemple d'un ensemble non-mesurable et le théorème de Cantor-Bendixson.

La notion générale de mesure (que par un changement d'échelle on peut toujours ramener à une mesure de probabilité) s'introduit sans ambiguité en prenant : mes. $([a, b[) = F(b) - F(a)$ F fonction non-décroissante de 0 à 1.

Un ensemble est probabilisable suivant F, si les F-mesures intérieures et extérieures coïncident. Les ensembles mesurables -B sont probabilisables quel que soit F.

L'exemple très détaillé de l'ensemble ternaire de Cantor illustre la décomposition de Lebesgue et Jordan de F.

L'intégrale de Lebesgue-Stieltjes s'introduit de la même façon que précedemment à partir de la mesure F et on établit le théorème de Riesz-Lebesgue.

L'ouvrage se termine sur l'examen des travaux d'E. Borel, relatifs à la raréfaction des ensembles de mesure nulle.

Section B : Statistique Mathématique

ANALYSE DE VARIANCE ET PLANS D'EXPERIENCE

Par
Daniel DUGUÉ et Maurice GIRAULT
- Dunod 1959 -
Analysé par J. LARRIEU

L'ouvrage de MM. Dugué et Girault se place dans la ligne de travaux consacrés en FRANCE à la statistique appliquée aux problèmes concrets. Il a pour but de préciser les méthodes qui permettent de rechercher d'une manière statistique les causes déterminantes dans les phénomènes physiques.

Un premier chapître est consacré au rappel des propriétés classiques de la loi normale et des lois qui en dérivent, loi de χ^2 de Student et de Behrens-Fisher, ceci pour les variables à une puis à plusieurs dimensions. On sait en effet que les seuls résultats exploitables obtenus jusqu'à présent en analyse de variance concernent les variables normales.

Dans un second chapître, les auteurs étudient l'analyse de la variance proprement dite, c'est-à-dire dans une population à plusieurs catégories la décomposition de la variance empirique en une somme de termes dont certains sont toujours des estimations de la variance vraie, les autres n'étant des estimations que si les diverses catégories sont homogènes en moyenne, la variance étant toujours supposée invariable dans les différentes catégories. Le problème est traité dans les cas où il y a un puis plusieurs facteurs contrôlés. La comparaison entre les différentes estimations fournit un test d'homogénéité des facteurs dans chaque catégorie.

Or, l'analyse de la variance classique exige de nombreux échantillons et par suite elle s'avère trop couteuse en de nombreux cas. C'est pourquoi les auteurs étudient ensuite les techniques de plans d'expérience qui ont pour but de diminuer la taille des échantillons nécessaires, ce qui perd évidemment une partie de l'information mais conserve l'essentiel. Le chapitre III contient la description d'un certain nombre de modèles (plans d'expérience) construits à partir des notions d'algèbre carrés latins, gréco-latins, blocs incomplets équilibrés. Les corps de Galois fournissent d'élégantes solutions à ces problèmes et donnent des solutions, sinon générales, du moins très intéressantes dans un certain nombre de cas précis.

L'ouvrage se termine par une série de tables numériques fort utiles au statisticien pour l'application des tests employés en analyse de variance.

Série C : Recherche Opérationnelle

INITIATION AUX PROCESSUS ALEATOIRES
LE PROCESSUS DE POISSON - FILES D'ATTENTE -
PANNES DE MACHINES

Par Maurice GIRAULT
Professeur à l'Institut de Statistique
Maître de Conférences à la Faculté des Sciences
de Caen
- Dunod 1959 -
Analysé par D. FOATA

Le présent ouvrage est une introduction à l'étude des processus aléatoires, mais c'est aussi, par ses nombreux exemples, un excellent guide pour les praticiens "désirant s'initier aux processus aléatoires et réfléchir à leurs utilisations". On y montre comment on peut donner à certains problèmes concrets tels que les files d'attente, les pannes de machines ... uné structure de processus aléatoire et comment ce schéma mathématique permet un bon calcul de l'optimum économique.

Le processus le plus simple et aussi le plus souvent rencontré dans la pratique est le processus de Poisson. Aussi est-il étudié en détail dès le début du livre. Il y a deux manières de le décrire : "soit donner la loi de probabilité de l'intervalle de temps qui sépare deux événements successifs, soit donner la loi de probabilité du nombre d'événements qui se produisent dans un intervalle de temps donné".

Plusieurs lois de probabilité dérivent de l'étude des processus de Poisson : fonctions eulériennes de première et de seconde espèce, loi de Poisson. L'auteur consacre donc un chapitre à l'étude de ces lois et aux liens qui existent entre elles.

Après avoir rappelé comment on peut tester l'hypothèse qu'un phénomène physique suit une loi de Poisson (test du χ^2), M. Girault montre, par deux exemples simples, comment on peut savoir si un système, qui évolue aléatoirement au cours du temps, atteindra ou non un régime permanent, "et si oui, avec quelle rapidité".

Puis on trouve une étude complète des processus d'engorgement et des files d'attente, dans les différents cas suivants :

- arrivées "poissonniennes" et durées de service exponentielles ; avec 1, 2, r postes de service.

- arrivées "poissonniennes" et durées de service constantes ; avec 1, 2 puis r postes de service.

- loi quelconque de durée et un poste de service.

Enfin, après quelques remarques sur les processus, l'auteur traite une série de problèmes et d'exemples.

IMPRIMERIE LOUIS-JEAN - GAP
Dépot légal : 171 — 1959